iCIO MAGAZINE

COMMUNITY MAGAZINE
AGUSTUS / 2018

Advanced Persistence Threat:
Pencuri dengan Kemampuan
Group Ocean's Eleven



YOU'RE HIRED!

Dalam Rapat Umum Anggota Mei 2018, Rico Usthavia Frans dipilih menjadi Chairman iCIO Community periode 2018 -2020 menggantikan Agus Wicaksono, Chairman periode 2016 -2018. Pada kesempatan yang sama juga telah dibentuk jajaran Pengurus iCIO Community periode 2018 -2020

9 772549 202009

iCIO COMMUNITY

JOIN US NOW VISIT OUR PAGE

www.ciocommunity.org

iCIO
COMMUNITY

SELAMAT BERTUGAS

Pengurus Perkumpulan Chief Information Officer Indonesia Periode 2018-2020



Rico Usthavia Frans | Jeny Mustopha | Dickie Widjaja | Debbie Nova | Dewi Saleh | YB Hariantono | Ivan Sangkereng | Novaldy Antonio | Danny Natalies | Lukas Djuanda | Hermawan Thendean | Abidin Riyadi Abie | Achmad Royhan | Jean H. Reksodiputro

INDEX 3

EDITOR'S COMMENT 4

KEPENGURUSAN ICIO COMMUNITY 2018-2022 5



THE BOARD OF COMMITTEE

CAPTURE 11

INSIGHT

Advanced Persistence Threat: Pencuri dengan Kemampuan group Ocean's Eleven 32

Siapkan BCP dan DR untuk Hadapi Ancaman Bencana 36

NEWS HIGHLIGHT

Blockchain: How Ready Are You? 15

Menelisik Prospek dan Dampak Pengembangan Blockchain 18

Konten Digital: Blockchain dan Rights Management 19

Paten: Melindungi Inovator dan Memberikan Insentif pada Inovasi 21

E-voting: Revolusi Sistem Elektoral 22

Smart Contracts: Ketika Kode Menjadi Hukum 24

Supply chains: Tingkatkan Transparansi dan Akuntabilitas 26

Blockchain States: Rethinking Public Services 28

STARTUP

Startup Makin Seksi Bisnis Venture Capital Tak Henti Berinovasi 39



iCIO MAGAZINE

Graha BIP Lt. 7
Jl. Jend. Gatot Subroto
Kav 23, Jakarta 12390
Telp. 021 5256088
www.iciocommunity.org
iCIO Community
@iCIOCommunity
iCIO Community

Editor
Tri Joko Susilo
tri.susilo@ciocommunity.org

Penasehat
Harry Surjanto
Rachmat Gunawan
Suzan Zhang
Suzan.Zhang@ciocommunity.org

Kontributor
Ovi Oktaviani

Produksi
Santi Marissa Laura
Committee@ciocommunity.org

Desainer Grafis
Zaki Ari Setiawan

Tentang iCIO Community

iCIO Community adalah komunitas CIO *(chief information officer)* dan staf senior di bidang TIK perusahaan dan organisasi di Indonesia. Komunitas ini didesikasikan untuk membantu para anggotanya menjadi pemimpin yang semakin efektif dan berkembang secara profesional maupun personal.

Tentang iCIO Magz

iCIOMagz menyajikan informasi terkait berbagai praktek-praktek terbaik dibidang TIK yang berkontribusi positif bagi perusahaan dan organisasi. Audiens iCIO Maz adalah CIO, CXO, akademisi hingga praktisi senior dibidang TIK yang bekerja di vendor- vendor produk dan solusi TIK

Agen Inovasi

Inovasi dibidang Teknologi Informasi (TI) merupakan salah satu yang berkembang pesat. Bagi para eksekutif bisnis, TI diyakini merupakan penentu hidup atau matinya industri yang kedua dalam tiga hingga lima tahun setelah faktor ekonomi. Kondisi itu tidak bisa dilepaskan dari peran TI dalam berkembang atau berakhirnya model bisnis, semakin kaburnya batas-batas antar industri dan perusahaan, serta tuntutan cara berpikir yang baru dalam menjalankan bisnis. Di tengah persaingan bisnis yang semakin brutal, peran chief information officer (CIO) sangat dibutuhkan perusahaan dan organisasi untuk mendorong inovasi dan mengadopsi TI yang diyakini para eksekutif akan berdampak besar untuk pertumbuhan bisnis dalam tiga hingga lima tahun ke depan.

Mendorong inovasi adalah prioritas utama dari strategi bisnis. Inovasi yang dibutuhkan perusahaan dan organisasi saat ini tidak berhenti hanya pada produk atau layanan, melainkan juga pada model bisnis hingga proses bisnis. Faktanya, disrupsi digital telah melahirkan para pemain baru diberbagai industri dengan model bisnis baru dengan cepat yang harus terus diantisipasi jika perusahaan tidak ingin terdisrupsi. Karena inovasi tidak akan pernah menunggu: dengan kata lain siapapun yang tidak mau atau mampu beradaptasi dengan perkembangan TI pasti akan tertinggal atau tergilas kompetisi.

Disrupsi digital ini juga menuntut CIO untuk beradaptasi dan terus mengembangkan kapasitas dan kapabilitasnya tidak hanya soal teknologi melainkan juga dibidang bisnis. Dengan latar belakang inilah iCIO Community dibentuk. 20 Mei lalu iCIO Community telah menginjak usianya yang kedua. Bertepatan dengan itu juga telah diselenggarakan Rapat Umum Anggota untuk memilih Chairman dan Kepengurusan baru periode 2018-2020.

Tentu semua anggota iCIO Community mengharapkan kepengurusan yang baru ini bisa melanjutkan kesuksesan yang telah dicapai kepengurusan sebelumnya dan meningkatkannya sehingga iCIO Community ini bisa benar-benar memberikan manfaat bagi seluruh anggotanya baik untuk perkembangan personal maupun profesional sehingga mereka selaku CIO bisa menjalankan perannya selaku agent of innovation di perusahaan dan organisasinya masing-masing. Semoga.



Tri Joko Susilo

Editor, iCIO Magz
iCIO Community

DUA TAHUN YANG MAKIN KRUSIAL

iCIO Community atau Perkumpulan Chief Information Officer (CIO) Indonesia mencapai milestone baru dalam sejarah organisasinya. Rapat Umum Anggota sebagai forum tertinggi organisasi pada Mei 2018 lalu telah memilih Kepengurusan Baru periode 2018-2020 untuk melanjutkan Kepengurusan Periode 2016-2018.

Pergantian Kepengurusan iCIO Community menjadi sebuah langkah penting dan krusial bagi organisasi dalam upayanya untuk merealisasikan misi iCIO Community menjadi komunitas para CIO dan eksekutif di bidang TIK perusahaan dan organisasi di Indonesia yang dapat menjadi wadah dan fasilitator pertukaran pengetahuan, peningkatan skill kepemimpinan, kontribusi untuk peningkatan IT capacity building secara nasional dan mitra pendorong pertumbuhan perekonomian.

Rico Usthavia Frans, yang baru terpilih sebagai Chairman iCIO Community periode 2018 – 2020 mengatakan peran pemimpin teknologi informasi (TI) tak lagi sebatas mengelola teknologi, tetapi juga mendukung kinerja bisnis, bahkan membangun keunggulan kompetitif perusahaan.

Menurut Rico perubahan peran CIO itu mulai terasa sekitar dua dekade seiring dengan perkembangan teknologi seperti IoT,Big Data, Cloud Computing, Artificial Intelligence, Machine Learning. Teknologi teknologi tersebut menjadikan berbagai proses bisnis antar unit bisnis dan pengambilan keputusan bisa dilakukan dengan lebih cepat. CIO pun mulai terlibat dalam semua aspek bisnis. Pada saat yang sama CEO pun mulai terbuka pandangannya terkait potensi teknologi untuk meningkatkan berbagai proses bisnis

"Jika di masa lalu kesuksesan CIO banyak dilihat dari sisi kemampuan dan kapabilitas terkait teknologi saja. Saat ini kesuksesan CIO dilihat dari sejauh mana mereka mampu memanfaatkan TIK untuk meng-*enable* proses bisnis, keterlibatannya dalam berbagai pengambilan keputusan startegis perusahaan dan mendorong profitabilitas bisnis," kata Rico.

Untuk itulah menurut direktur teknologi informasi dan operasi, PT. Bank Mandiri Tbk, CIO pemimpin TI tentu tak bisa berdiam diri. "Salah satu cara mengkomodasinya, bergabung dengan iCIO Community, yang anggotanya terdiri dari IT leader dari berbagai industri dan latar belakang," kata Rico.

Profesi CIO kini menjadi ujung tombak perusahaan di era disrupsi digital. Urgensi penguatan iCIO Community sebagai organisasi profesi para pengambil keputusan di bidang TIK menjadi semakin krusial.

Bergabung dengan iCIO Community menurut Rico akan mempermudah para CIO untuk berbagai pengalaman dan membangun networking. Dengan anekaperan barunya, seorang pemimpin TI membutuhkan wadah untuk memfasilitasi sharing berbagai ide terkait, antara lain, teknologi dan best practices. Rico yakin dengan berada di tengah komunitas ini, para pemimpin TI belajar beradaptasi dan mengasah kemampuannya terkait berbagai prioritas bisnis, serta membangun relasi bisnis yang lebih baik.

"Kebutuhan bisnis dan pelanggan yang semakin besar akan teknologi menuntut para pemimpin TI untuk mengeksplorasi aneka cara baru untuk berkontribusi pada industri maupun masyarakat yang lebih luas. iCIO Community membuka kesempatan terbaik bagi para CIO untuk bertukar pengetahuan, skill, dan pengalaman dengan industri dan masyarakat lainnya sehingga IT leader dapat menemukan cara baru untuk menjawab aneka tantangan dari industri," tambah Rico.

Penguatan Organisasi

Agar iCIO Community bisa menjadi wadah yang bisa memenuhi kebutuhan anggotanya selaku Chairman terpilih Rico bertekad melanjutkan kinerja kepengurusan sebelumnya. Selain itu untuk memperkuat organisasi, ia dan segenap pengurus sepakat untuk menambahkan satu pilar, yakni Research, untuk melengkapi empat pilar organisasi yang sudah ada (Membership, Advokasi, Komunikasi, dan Partnership).

"Harapannya tentu saja (agar iCIO Community) bisa terus mendorong dan meningkatkan benefit bagi member khususnya, dan masyarakat yang lebih luas pada umumnya," jelasnya.

Tentu saja tidak mudah untuk mencapai hal tersebut. Untuk itu Rico menghimbau agar semua anggota berpartisipasi secara aktif dalam setiap *event* atau aktivitas yang diselenggarakan iCIO Community, sehingga para anggota benar-benar dapat merasakan manfaat optimal dari komunitas ini. Dan tentu saja di antara manfaat tersebut adalah mendukung para pemimpin TI dalam menjalankan peran-peran barunya.

"Saya juga ingin mengundang para CIO dan Eksekutif di bidang TI dari organisasi maupun perusahaan di Indonesia untuk bergabung dengan sekitar dua ratus anggota kami saat ini untuk bersama-sama mengembangkan komunitas inimenjadi representasi yang kuat dari profesi CIO di Indonesia," tuturnya.

Profil Pengurus iCIO Community periode 2018 – 2020



Rico Usthavia Frans merupakan Direktur Teknologi Informasi dan Operasi PT. Bank Mandiri Tbk. Rico dipilih anggota iCIO Community untuk menjadi Chairman dalam Rapat Umum Anggota yang berlangsung pada Mei 2018 lalu. Sebelumnya pria yang menamatkan kuliahnya di jurusan Teknik Elektro Institut Teknologi Bandung ini dipilih oleh para Juri iCIO Awards 2018 sebagai pemenang kategori "The Most Influential CIO" pada April 2018. Sebelum memasuki karir profesionalnya di industri perbankan tepatnya di Citibank, Rico memulai karir profesionalnya di industri perminyakan. Setelah 5 tahun meniti karir di Citibank dengan posisi terakhir sebagai Country Marketing Manager, pada 2010, Rico bergabung di Bank Mandiri sebagai Group Head Electronic Banking (2010-2013) dan SEVP Transaction Banking
(2013-March 2016).

RICO USTHAVIA FRANS



Jeny kembali dipercaya untuk menjadi pengurus iCIO Community periode 2018 – 2020. Jika pada Kepengurusan periode 2016 – 2018, Jeny diberikan amanah untuk menjadi salah satu Koordinator di Divisi Membership, kali ini Jeny dipilih untuk mengemban tugas sebagai Sekertaris Jenderal. Karir profesional Jeny saat ini adalah Chief of Information Technology Services Commonwealth Life dan bertanggung jawab untuk menjalankan visi dan memimpin Transformasi di IT dengan inisiatif-inisiatif baru di Department IT. Memulai karirnya di industri keuangan sejak 1986 dan Jeny Mustopha terakhir menjabat sebagai Head of Business Transformation of Allianz Life. Jeny pernah menduduki posisi VP IT Strategy di PT Garuda Indonesia, PT AXA Services Indonesia, serta IT Division Head (CIO) of PT Asuransi Astra Buana, VP IT Devision Head Application Development and Business Alliance of PT Bank Universal, dan System Analist di PT Bank Danamon Indonesia. Memilik kualifikasi Sarjana Business Computing System dan gelar diploma Business Associate dari Stanford College, Malaysia

JENY MUSTOPHA



DICKIE WIDJAJA

Lulusan S1 University of Michigan, Ann Arbor, ini dipilih sebagai Bendahara Kepengurusan periode 2018 – 2020. Dickie mulai meniti karirnya di bidang TIK di negeri Paman Sam sebagai Database Administrator dan kemudian ditempatkan di Indonesia sebagai Regional Content Manager Lycos Asia. Dickie kemudian mengembangkan karirinya dan dipercaya menjadi Head of Portal e-Channels oleh AstraWorld yang bertanggung jawab untuk mengelola website semua Astra Group yang didedikasikan untuk pelanggan. Setelah malang melintang di industri TIK selama lebih kurang 15 tahun Dickie mencari tantangan baru dengan bergabung di Investree, sebuah perusahaan rintisan dibidang keuangan yang memiliki misi untuk menjadikan industri pembiayaan menjadi lebih aman dan mudah.



DEBBIE NOVA

Rapat Umum Anggota 2018, kembali mempercayai Debbie sebagai Pengurus iCIO Community periode 2018 – 2020. Ini kali kedua setelah dua tahun sebelumnya ia menduduki posisi yang sama. Di Kepengurusan periode lalu, Debbie menjadi koordinator yang bertanggung jawab dalam bidang Membership untuk membuat ketentuan keanggotaan iCIIO Communty, perekrutan anggota baru dan juga pengembangan organisasi. Saat ini Debbie adalah Group Chief Information Officer Coca-Cola Amatil. Jabatan itu telah dipegangnya sejak Januari 2018. Alumni Universitas Trisaksi jurusan Teknik Industri ini sejak menyelesaikan pendidikannya merintis dan meniti karir di Coca Cola sejak 1996 sebagai National IS&T Manager Coca-Cola Bottling Indonesia hingga posisi tertinggi di bidang TIK di perusahaan kelas dunia itu.



YB HARIANTONO

Pada Rapat Umum Anggota 2018, Pria kelahiran Malang, Jawa Timur ini didaulat menjadi salah satu koordinator bidang Membership, Kepengurusan periode 2018 – 2020. Sepanjang karirnya lulusan Teknik Elektro, Institut Teknologi Sepuluh Nopember Surabaya di habiskan di industri perbankan. Memulai karir pada tahun 1991 di Bank Bali dan sempat menjabat sejumlah posisi sampai dengan tahun 2002 pada 2003, YB Hariantono bergabung dengan Bank Permata.Di Bank yang dimiliki oleh Grup Astra, YB bertahan hingga tahun 2010 dengan menjabat berbagai posisi seperti Head of Network, Head of Special Project, Head of IT, dan Head of Consumer Credit Underwriting. Pada tahun 2010 bergabung dengan MayBank - BII sebagai EVP, Head IT hingga tahun 2014. Pada Maret 2014 menjabat sebagai Direktur Operation & IT di Bank Mega hingga saat ini.

Kepengurusan iCIO Community 2018 -2020



Rapat Umum Anggota 2018 memilih Dewi T Saleh, IT Director PT. Kawan lama Sejahtera menjadi salah satu Koordinator Divisi Membership periode 2018-2020. Jebolan Master di bidang Matematika Wichita State University ini sebelumnya pernah menjabat Senior Manager dan Inclusion and Diversity Lead di Accenture Indonesia.

DEWI T. SALEH

LUKAS DJUANDA

CIO PT. Japfa Comfeed IndonesiaTbk ini kembali dipercaya untuk menjadi salah satu Pengurus periode 2018 – 2020. Seperti pada periode 2016 – 2020, Lukas dipilih untuk menjadi salah satu Coordinator Communications Division.





Danny terpilih terpilih menjadi koodinator Divisi Communication pada Rapat Umum Anggota 2018 – 2020. Saat ini karir profesional Danny adalah sebagai CIO di Universitas Katolik Atmajaya, Jakarta. Sebelum menjadi CIO di almamaternya, lulusan Fakultas Teknik Ilmu Komputer Universitas Atmajaya ini meniti karirnya di bidang TIK berbagai perusahaan dengan latar belakang industri yang berbeda-beda. Danny memulai karirnya sebagai admin IT Network di Total Bangun Persada mulai 2005 hingga 2006. Karirnya kemudian berlanjut di Bright Little Stars Limited, PT. JJ Multi Utama Indonesia, PT. Gunung Subur Sejahtera hingga kemuadian menempati posisinya yang sekarang di Atmajaya sejak 2010.

DANNY NATALIES



NOVALDY ANTONIO

Rapat Umum Anggota 2018 kembali mengukuhkan Novaldy sebagai salah satu koodinator Divisi Partnership Kepengurusan periode 2018 – 2020. Sebelumnya pada Kepengurusan periode 2016 – 2018, pemegang gelar S1 dari RMIT University Australia ini juga mengemban amanah di posisi yang sama. Saat ini Novaldy menjabat sebagai Senior Manager Information Technology Services di Rumah Sakit Pondok Indah Group dan Equity Partner di perusahaan konsultan TIK-Veda Praxis . Karirnya di TIK telah dimulai pada tahun 2000 dengan menjadi IT Auditor di Ernst & Young. Setelah selama 5 tahun menjadi IT Auditor, Novaldy melanjutkan karirnya di Adira Finance dan menduduki jabatan sebagai Head of IT QA & Compliance. Pada 2013 Novaldy mulai bergabung dengan RS Pondok Indah sebagai IT Project & Compliance Development Manager.



IVAN SANGKERENG

Salah satu Koordinator Divisi Communications periode 2016 – 2018 ini kembali dipercaya untuk mengemban amanah di Kepengurusan periode 2018 – 2020. Berbeda dengan periode sebelumnya, Ivan saat ini dipercaya untuk memperkuat Divisi Partnership. Saat ini Ivan menjabat sebagai CIO di Bina Nusantara Group. Penyandang gelar S1 Teknik Elektro Universitas Hasanudin dan MM dari Binus Business School ini memiliki pengalaman cukup lengkap di berbagai sektor industri. Pada Tahun 2000, Ivan memulai karirnya di dunia TIK dengan menjadi Software Manager di PT. Arta Boga Cemerlang -Orang Tua Group. Di perusahaan ini karirnya berkembang hingga menduduki posisi CIO 2003 – 2005. Setelah hampir lima tahun terjun di industri ritel, Ivan menjajal kemampuannya di industri otomotif dan bergabung sebagai Business Operation Head di Asco Automotive. Di sana Ivan bertahan 5 tahun dan kemuadian melanjutkan karurnya di PT. Green Planet selama setahun dan kemudian dipercaya menjadi IT



JEAN H. REKSODIPUTRO

Jean kembali diberi amanah oleh Rapat Umum Anggota 2018 untuk menjadi koordinator bidang advokasi periode 2018 – 2020. CIO dari PT. Pefindo Credit Bureau ini pada periode sebelumnya juga dipercaya menjabat posisi yang sama. Sarjana di bidang MIS dari Universitas Gunadarma ini merintis karir di bidang TIK di berbagai perusahaan yang bermarkas di Amerika Serikat. Tahun 1999 - 2000, Jean bekerja sebagai programmer di SDI Technology Inc, di Pitsburg. Pada 2001 hingga 2003 ia bekerja sebagai Senior Programmer/Analyst di Weidenhammer Systems Corporation di Pensylvania. Sebelum kembali ke tanah air pada 2014 setelah ditunjuk menjadi CIO di Pefindo, Jean masih berpindah-pindah ke sejumlah perusahaan di Amerika hingga 2013.



Vice President Information Technology PT. Citilink Indonesia, ini oleh Rapat Umum Anggota diberi amanah untuk bergabung di dalam Kepengurusan periode 2018 – 2020 tepatnya untuk menjadi Koodinator di Divisi Advokasi. Sarjana Sistem Informasi STIKOM ini telah menghabiskan karirnya selama satu dekade terakhir di Citilink. Beragam posisi di bidang TIK dijalaninya di perusahaan penerbangan itu mulai dari IT Systems Analyst September 2008 – September 2013, IT Application Senior Manager September 2014 – September 2015 hingga VP Information Technology yang diembannya sejak Oktober 2013 hingga saat ini.

ACHMAD ROYHAN

Abidin terpilih sebagai sebagai salah satu Koordinator Divisi Research periode 2018 – 2020. Jebolan Universitas Gadjah Mada menjalani karirnya yang panjang di bidang TIK di Astra Group. Abidin pernah menduduki posisi sebagai SAP Basis & Support Head mulai sepanjang 1998, lalu IT Operation Head 1999 – 2000 di PT. Astra International. Masih Astra Group mulai 2000 – 2006, Abidin aktif di Astra Graphia Informasion Technology sebagai Outsourcing Services Division. Mulai 2006 hingga saat ini Abidin diberi tugas di PT Toyota Astra Financial Services mulai dari IT Division Head hingga IT & GA Division Head.



ABIDIN RIYADI ABIE



HERMAWAN THENDEAN

Execuitve Vice President PT. Bank Central Asia Tbk ini diberikan amanah pada Rapat Umum Anggota 2018 untuk menjadi Koordinator Divisi Research yang baru dikembangkan pada Kepengurusan periode 2018-2020. Penyandang gelar S1 dari San Fransisco State University pada 1985 dan MBA dari Golden State University pada 1986 ini sebelumnya menjabat sebagai IT General Manager BCA mulai 2007 hingga 2014.



Milenial Pesimis Terhadap Dunia Bisnis

Sebanyak 25 persen generasi milenial di Asia Tenggara menunjukkan sikap pesimistis dalam menghadapi Industri 4.0. Mereka menginginkan dunia bisnis berkontribusi terhadap masyarakat luas. Fakta ini terungkap dalam Survei Milenial Tahunan 2018 yang diselenggarakan oleh Deloitte, perusahaan multinasional yang bergerak di bidang keuangan, konsultan, dan manajemen.Survei tahunan Deloitte ini melibatkan 10.455 responden kaum milenial dan hampir 1.850 responden generasi Z di 36 negara-generasi milenial lahir pada 1977-1995, sedangkan generasi Z pada pertengahan 1990-2000an. Menurut Deloitte survei ini menunjukkan para pebisnis tidak dapat lagi melakukan business as usual. Pandangan skeptis para milenial menuntut para pemimpin bisnis mampu keluar dari zona nyaman, dan melihat lebih kritis lagi cara kerja dalam bisnis masing-masing beserta dampak positif yang diberikannya, baik bagi karyawan maupun dunia secara lebih luas.



Platform Lowongan Kerja Berbasis Blockchain di Luncurkan

Proyek ambisius ChronoBank membangun sebuah platform lowongan kerja yang sepenuhnya berbasis teknologi Blockchain akhirnya rampung dengan peluncuran LaborX baru-baru ini. LaborX saat ini menjadi bagian paling penting dari ekosistem human resource ChronoBank, memberikan para pencari kerja dan perusahaan untuk bertansasksi secara cepat, aman, dan efektif. Dengan peluncurannya ini LaborX menjadi aplikasi pertama berbasisi Blockchain yang sah siap untuk diadopsi secara massal. LaborX diklaim mampu memangkas biaya pencarian kerja dan biaya penggunaannya hanya mencapai 1 % - jauh lebih murah dibanding standar saat ini yang berkisar 5 % - 20% . Saat ini Edway Training dan DGTek sudah mulai memanffatkan platform ini.



Supply Chain Menjadi Sasaran Serangan Siber

Laporan Dimension Data, perusahaan jasa di bidang teknologi menyebutkan supply chain telah menjadi target serangan siber saat ini. Pada 2017, tercatat 20% serangan siber mengarah ke supplay chain lebih besar dari sektor teknologi 19%, sektor bisnis dan layanan profesional sebesar 10 % serta hanya kalah dari sektor keuangan yang menjadi target serangan ransomware sebesar 26%. Laporan tersebut juga mengungkapkan mengapa supply chain kini menjadi target serangan khususnya ransomware adalah karena karena terdapat pertukaran informasi yang bisa dimanfaatkan untuk melakukan pencurian data. Data yang dicuri bisa berupa data konsumen, rekaman transaksi atau tentang substansi masalah tertentu bila dikaitkan pada sektor bisnis dan layanan profesional. Secara total, sepanjang 2017 terjadi 150 juta serangan. Dengan angka ini, setidaknya terjadi 3 juta serangan per minggu atau sekitar 50.000 serangan per hari di seluruh negara.



Microsoft Coba Bangun Data Center Bawah Laut

Baru-baru ini Microsoft menurunkan sebuah prototype data center di laut sekitar pulau Orkney Skotlandia. Prototipe data center itu memuat 12 rack untuk sekitar 864 server dan sistem pendinginan. Sebelumnya prototipe itu dirancang dan diuji di Perancis sebelum dibawa ke Skotlandia dan diturunkan di kedalaman 117 feet dari permukaan laut. Pasokan listrik data center tersebut disediakan oleh European Marine Energy Center yang mengandalkan turbin dan energi angin untuk mendorong listrik yang berasal dari gelombang laut.Pada kapasitas maksimalnya data center tersebut hanya membutuhkan seperempat megawatt. Sebelumnya Microsoft juga telah membangun prototipe data center bawah laut di kawasan pantai California pada 2015



Komisi Eropa akan Denda Google

Dalam beberapa tahun terakhir, Google harus menghadapi tiga tuntutan kasus yang dilakukan oleh Komisi Eropa pada Google Shopping, AdSense, dan dominasi Android di pasar smartphone. Tuntutan terkait Android kemungkinan besar akan dilakukan pada Juli tahun ini. Para ahli memperkirakan nilai pinalti yang harus ditanggung Google dengan tuntutan tersebut jauh lebih besar dari yang harus dibayarkan Google tahun lalu sebesar US $ 2.8 milyar. Masalah yang dihadapi Google ini dimulai pada 2016, ketika Komisi Eropa menuduh Google memanfaatkan Android untuk mempertahankan posisinya terkait pencarian di internet termasuk meminta produsen smarphone untuk pre-install Google browser. Selain itu Google juga dituduh memberikan insentif keuangan bagi produsen smartphone yang mau melakukannya.



Indonesia akan Mengatur Mata Uang Digital Sebagai Komoditas

Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) segera merilis aturan perdagangan mata uang kripto bitcoin sebagai produk komoditas. Keputusan tersebut berdasarkan kajiannya bersama Universitas Indonesia yang menyimpulkan tidak melanggar Undang-Undang tentang Perdagangan Berjangka. Meski saat ini hasil kajian tersebut masih perlu di revisi, namum Bappebti optimis aturan terkait perdagangan bitcoin sebagai komoditas ini siap dalam waktu dekat. Jika aturan tersebut telah diluncurkan maka Bitcoin bisa diperdagangkan seperti layaknya perdagangan emas. Uang kripto ini perlu diatur untuk memberikan perlindungan kepada konsumen. Dalam hal pajak, pengaturan ini juga akan membuat semakin transparan dan terpenting dengan aturan tersebut bisa mencegah pencucian uang. Saat ini nilai transaksi bitcoin di Indonesia sudah mencapai Rp. 1 trilliun dalam sehari.



Data Governance: Sisakan Sejumlah Tantangan Bagi CIO

Peningkatan tata kelola data dalam beberapa tahun tahun terakhir terus menjadi agenda utama para CIO. Meski demikian sejumlah tantangan masih menghadang.

Hal tersebut terungkap dalam sebuah diskusi yang diselenggarakan oleh iCIO Community di Jakarta beberapa waktu lalu. Para *chief information officer* (CIO) dan eksekutif dibidang TIK dari berbagai industri mulai perbankan, asuransi, manufaktur, kesehatan, *oil & gas* mengakui upaya meningkatkan tata kelola data yang telah dilakukan dalam beberapa tahun terakhir ini belum mendapatkan hasil yang menggembirakan. Akibatnya data yang dimiliki perusahaan dan organisasi belum bisa dimanfaatkan secara optimal untuk memperoleh *insights* yang diharapkan bisa membantu mengambil berbagai keputusan strategis.

Sejumlah tantangan masih menghadang dan berbeda pada setiap industri. Namun secara garis besar berbagai tantangan tersebut terbagi dalam empat kategori, yakni mendefinisikan strategi tata kelola data, infratruktur teknologi informasi dan komunikasi yang dibutuhkan, dukungan dari *stakeholder* khususnya top level manajemen, dan meminimalkan resiko dan keamanan data.



"Untuk membangun daya saing, di era disrupsi digital ini menuntut perusahaan dan organisasi lebih responsif dan adaptif terhadap perubahan. Untuk itu perusahaan membutuhkan informasi yang akurat berdasarkan data-data yang bisa dipertanggungjawabkan," kata Agus Wicaksono," Chairman iCIO Community. Namun kualitas data sangat ditentukan oleh bagaimana praktik-praktik tata kelola data diterapkan. Dan ini masih menjadi pe er utama para CIO tidak hanya di Indonesia tetapi juga di negara-negara lain.

Menurut Agus hal inilah yang menjadi latar belakang diselenggarakannya diskusi."Kami ingin memfasilitas para member untuk saling berbagi pengalaman dan best pratice terkait pengembangan *data governance*.

Debbie Nova, CIO Coca Cola Amatil yang terlibat mengaku diskusi terkait pengembangan data governance tersebut sangat bermanfaat. Para peserta diskusi bisa saling belajar satu sama lain dan men-*challenge* inisiatif pengembangan tata kelola data yang telah dilakukannya untuk menjadi lebih baik lagi. " Saya ingin diskusi-diskusi seperti ini terus ada dan kalau bisa intesitasnya ditingkatkan di masa-masa mendatang."



Blockchain: How Ready Are You?

Seperti halnya Internet, Blockchain diyakini akan membawa perubahan yang besar bagi perusahaan dan organisasi dalam menjalankan roda bisnisnya. Namun, berdasarkan Gartner CIO Agenda Survey 2018 yang melibatkan 3160 CIO di seluruh dunia baru-baru ini, hanya satu persen CIO yang telah mengadopsinya dan sekitar delapan persen baru memiliki rencana untuk mengimplementasikannya.

David Furlonge, vice president and Gartner Fellow menduga alasan dibalik itu adalah karena *value proposition* teknologi blockchain tidak diartikulasikan dengan baik, sehingga kalangan bisnis tidak memahami manfaatnya secara jelas, seperti halnya teknologi lain yang ada di pasar saat ini.

"Apa proposisi nilai untuk blockchain dalam konteks perusahaan? Inisiatif interoperabilitas antara *ledger* dan antara sistem *non-blockchain* dan *ledger* itu belum matang. Dan masih banyak hal lain ini yang membuat CIO belum meyakini untuk mengubah prioritas ke teknologi blockchain," kata David

Fakta lainnya, kata David adalah kesiapan dan kapabilitas enterprise untuk mengadopsi blockchain dan model bisnis baru/ operasionalnya masih sangat terbatas.

"Para eksekutif bisnis membutuhkan lebih banyak waktu untuk lebih memahami apa itu blockchain dan bagaimana penerapannya dalam konteks bisnis maupun teknologi mereka."

Fakta lain mengkonfirmasi hal tersebut. Sepanjang 2017 hingga awal 2018 "blockchain" merupakan terminologi yang paling banyak dicari di situs Gartner Inc. Hal itu diungkapkan oleh Jon Krause, vice president & executive partner, Gartner Executive Partner pada acara CTI IT Infrastructure Summit 2018 di Jakarta beberapa waktu lalu. Dalam acara yang bertajuk "Blockchain: The Next Digital Revolution in Every Industry, tersebut Jon Krause mengungkapkan fokus utama pencarian para eksekutif adalah terkait vendor, acara dan event, hingga hasil



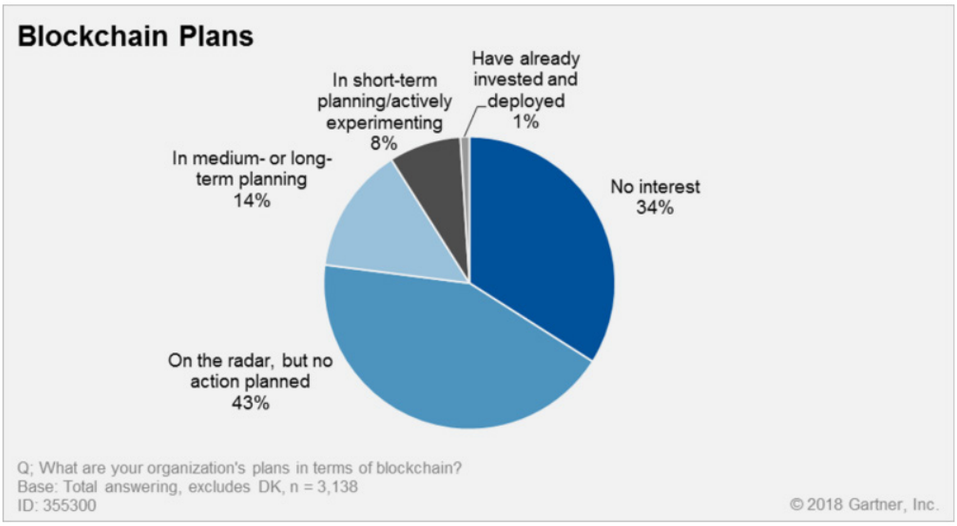
Jon Krause
Vp & Executive Partner, Gartner Executive Partner

penelitian terkait membangun business cace untuk proyek blockchain.

"Kami harus merespon begitu banyak pertanyaan dari kalangan eksekutif terkait apakah blockchain itu, bagaimana teknologi blockchain bisa di aplikasikan pada bisnis mereka hingga bagaimana perusahaan dan organisasi memperoleh value dari penerapan teknologi blockchain," kata Jon.

Penuh Tantangan

Hasil Gartner CIO Agenda Survey 2018 itu pula mengungkapkan bahwa dari 293 CIO organisasidan perusahaan yang dalam waktu dekat ini akan mengimplementasikan dan atau telah menggelar inisiatif



Sumber: Gartner (Mei 2018)

penerapan teknologi blockchain ini, dua puluh tiga persennya mengungkapkan blockchain membutuhkan *skill* yang benar-benar baru, dan empat belas persennya mengeluhkan sulitnya mendapatkan *talent* yang memiliki *skill* yang dibutuhkan. Sementara empat belas persen lainnya mengindikasikan bahwa penerapan blockchain menuntut perubahan budaya kerja dan tiga belas persen CIO mengungkapkan kebutuhan perubahan struktur kerja di departemen TI.

"Para CIO menyadari bahwa penerapan blockchain akan mengubah model operasi maupun bisnis organisasi dan mereka optimis bisa mengatasi tantangan tersebut," kata David melalui siaran persnya. Penerapan teknologi blockchain menuntut pemahaman menyeluruh mulai dari berbagai aspek keamanan, hukum, *value exchange*, tata kelola yang terdesentralisasi, hingga proses dan arsitektur komersial," kata David.

Dari sisi industri, CIO berlatar belakang industri telekomunikasi, asuransi dan layanan keuangan menjadi yang paling aktif dalam perencanaan dan ujicoba teknologi blockchain dibandingkan dari industri lainnya. Sektor lain seperti transportasi, utilitas, dan pemerintahan juga terus meningkat perhatiannya pada teknologi ini karena fokus mereka adalah mendorong efisiensi dan membidik peluang *supply chain* serta logistik.

Meski mayoritas CIO belum memiliki rencana untuk mengadopsi blockchain dalam waktu dekat, sejatinya mereka telah memahami potensi disrupsi dari teknologi berplatform terbuka dan *shared ledger* ini. Apalagi semakin hari model pemanfaatannya (*use case*) juga semakin bertambah. Aplikasi-aplikasi blockchain untuk berbagai industri mulai banyak tersedia. Sebagai contoh,salah satu pelabuhan terbesar di dunia, yakni Rotterdam telah membangun sebuah lab untuk mengeksplorasi aplikasi-aplikasi blockchain untuk logistik, Sektor utilitas di kawasan Amerika Utara dan Eropa mulai menggunakan blockchain untuk perdagangan energi masa depan dan mengelola pembayaran di stasiun pengisian bahan bakar listrik. Tak ketinggalan solusi-solusi untuk enterprise yang terus dikembangkan oleh Konsorsium Blockchain – termasuk Enterprise Ethereum Alliance, Hyperledger Project, R3, and B3i.

Berbagai inovasi aplikasi berbasis blockchain itu akan terus bertambah. Gartner Inc. memproyeksikan bahwa nilai tambah bisnis blockchain akan tumbuh menjadi US176 miliar dolar pada tahun 2025.

Siapkan Standardisasi

Terus berkembangkan pemanfaatan blockchain baik dari sisi cakupan, skala, dan kompleksitasnya, kebutuhan akan teknologi, platform, dan skill yang terstandardisasi menjadi semakin mendesak. Firma konsultan terkemuka di dunia, Deloitte mengungkapkan empat alasan mengapa standarisasi sangat penting. Pertama, enterprise menjadi lebih mudah berbagi solusi dan kolaborasi dalam proses pengembangan aplikasi; kedua teknologi yang distandarisasi bisa terus; ketiga, enterprise bisa menggunakan standarisasi untuk memvalidasi PoC mereka serta memperluas standar tersebut di seluruh organisasi; dan keempat, *talent -talent* di industri TI memiliki kesempatan untuk mengembangkan pengetahuan mereka secara lebih komplit pada satu hingga 2 protokol / platform blockchain dibandingkan menguasai *knowhow* banyak platform.

Faktanya saat ini belum ada satu pun standar teknis yang lengkap untuk blockchain, dan tidak ada jaminan apapun hal itu akan segera tersedia dalam waktu dekat. Termasuk

untuk *use case* yang saat ini gencar dilakukan di seluruh dunia.

Pertanyaannya adalah apakah Anda – CIO dan tim bekerja untuk menentukan standar sendiri atau diam dan menunggu pesaing-pesaing Anda membangun standar itu?

Bagi JP Morgan Chase, menunggu para kompetitornya untuk menciptakan standar blockchain bukanlah pilihan. Pada 2017 lalu, perusahaan penyedia layanan keuangan terkemuka di dunia itu meluncurkan Quorum, *open-source*, *enterprise – ready distributed ledger*, dan platform smart contracts yang dibuat khusus untuk memenuhi kebutuhan industri jasa keuangan. Keunikan desain Quorum saat ini masih dalam terus dalam tahap pengembangan dan JP Morgan mengundang ahli teknologi dari seluruh dunia untuk berkolaborasi dalam pengembangan solusi tersebut.

Tentu saja langkah JP Morgan untuk mengembangkan standar blockchain itu tidak harus diikuti mentah-mentah. Tetapi Deloitte menyarankan ada langkah-langkah yang dapat dilakukan CIO untuk mempromosikan standardisasi dalam perusahaan dan industri mereka dibandingkan hanya dian dan pasif menunggu standar universal yang muncul. Misalnya, dengan mulai membangun hubungan dengan mendorong diskusi standardisasi dan bertukar *best practice* dengan organisasi yang berpikiran sama. Secara internal, CIO mulai dapat memberdayakan tim mereka untuk membuat keputusan yang mendorong standarisasi dalam ekosistem perusahaan. Terakhir di setiap organisasi manajemen data dan proses standar pastinya sudah ada. Terapkan standar yang sama pada solusi blockchain Anda. *So, how ready are you?*

Milestones Perkembangan Blockchain

- Bitcoin: Merupakan inovasi utama di awal-awal perkembangan blockchain dan bahkan orang lebih mengenal bitcoin itu sendiri dibanding blockchain Saat ini mata uang digital ini memiliki nilai pasar sekitar US 104 milyar dolar lebih dan digunakan oleh jutaan orang sebagai sistem pembayaran, termasuk untuk pasar Remittance yang nilainya terus berkembang.

- Inovasi tahap kedua sering disebut blockchain, yang digunakan untuk menggambarkan realisasi dari teknologi itu sendiri yang menjadi basis dari bitcoin dan dibedakan dari mata uang serta mulai digunakan dalam berbagai bentuk kerjasama antar organisasi. Saat ini mayoritas institusi keuangan di dunia sedang melakukan penelitian blockhain.

- Perkembangan tahap ketiga dari teknologi blockchain ini diidentikkan dengan perkembangan *smart contract*, yang merupakan bagian dari sistem blockchain generasi kedua-Ethereum. Ethereum merupakan program komputer yang dikembangkan dalam blockchain yang memungkinkan instrumen keuangan, seperti produk pinjaman dan obligasi dapat diwakili, berbeda dengan bitcoin yang menggunakan *token*. Platform *smart contract* ethereum saat ini memiliki nilai pasar milyaran dolar, dan ratusan proyek pengembangannya siap diluncurkan ke pasar.

- Inovasi generasi keempat blockchain diidentikan dengan pengembangan "*proof of stake*". Selama ini sistem pengamanan blockchain dikenal dengan sebutan "*proof of work*", yakni grup *miner* yang terhubung dalam jaringan komputer sebagai pengambil keputusan. Miners mengoperasikan data center yang menjadi sistem keamanan dalam transaksi pembayaran mata uang digital. "*Prove of stake*" adalah peningkatan dari *miner* dan kabarnya siap *go-live* dalam waktu dekat ini.

- Generasi kelima inovasi blockchain identik dengan pengembangan *blockchain scaling*. Saat ini di dunia blockchain setiap komputer dalam jaringan terlibat dalam pemmrosesan setiap transaksi. Hal itu menyebabkan prosesnya berjalan lambat. *Blockchain scaling* akan mempercepat proses tersebut tanpa mengorbankan faktor keamanan, melalui pemetaan jumlah komputer yang sesungguhnya dibutuhkan untuk melakukan validasi sebuah transaksi dan mengelompokkannya sendiri agar menjadi lebih efisien. Untuk mengelolanya tanpa mengorbankan faktor keamanan dan kehandalan blockchain itu bukan hal yang mudah, tapi tidak berarti mustahil. Dalam sekali proses kerjanya *blockchain scalling* ini diharapkan bisa secepat proses kerja dalam Internet of Thing dan mirip dengan sistem pembayaran terkemuka di dunia seperti VISA.

- Blockchain hari ini dan setiap inovasi yang telah dikembangkan dimulai sejak satu dekade yang lalu dan mayoritas dilakukan oleh sekelompok ilmuan komputer, kriptografer dan matematikawan.

Menelisik Prospek dan Dampak Pengembangan Blockchain

Seperti Internet di awal masa-masa perkembangannya, teknologi Blockchain sangat rumit untuk dipahami dan diprediksi arah pengembangannya. Departemen Penelitian Parlemen Eropa (European Parliamentary Research Service) merilis laporan terkait prospek dan dampak pengembangan teknologi ini.

Jika ada *disruptive technology* yang begitu banyak menyita perhatian berbagai kalangan, terutama para pengambil keputusan, Blockchain adalah salah satunya. Sejak diperkenalkan oleh Satoshi Nakamoto, lewat tulisannya yang bertajuk "*Bitcoin: A Peer to Peer Electronic Cash System*", pada tahun 2008, teknologi blockchain langsung menarik perhatian publik. Teknologi yang dideskripsikan oleh pria yang identitas aslinya masih misterius hingga saat ini sebagai "*purely peer-to-peer version of electronic cash*" itu kemudian lebih dikenal sebagai Bitcoin. Sally Davies, jurnalis teknologi di Financial Time, menyebut blockchain adalah Bitcoin, seperti Internet adalah email, yakni sebuah sistem elektronik raksasa, yang diatasnya memungkinkan dibangun berbagai aplikasi, dan mata uang hanya menjadi salah satunya.

Hari ini atau satu dekade sejak diperkenalkan, masih banyak orang percaya bahwa Bitcoin dan blockchain itu sama dan satu. Meski demikian sejak 2014 sudah mulai banyak perusahaan atau organisasi yang berani melakukan investasi untuk menelisik potensi pengembangan dari blockchain tersebut.

Salah satu institusi yang secara serius melakukan hal itu adalah Parlemen Eropa. Melalui unit penelitiannya-European Parliamentary Research Services (EPRS) mereka telah merilis laporannya dengan tajuk "*How Blockchain Could Change Our Live*" 2017. Menurut laporan tersebut ada banyak potensi pemanfaatan teknologi blockchain di luar implementasinya di bidang mata uang digital yang sudah populer. Meski demikian implikasinya juga harus diantisipasi karena bisa menabrak aturan yang sudah ada dan pada akhirnya justru menimbulkan kerugian khususnya bagi pelanggan dan masyarakat yang lebih luas.

Sebagai gambaran besar, EPRS menyebutkan bahwa keunggulan yang ditawarkan mata uang digital berbasis blockchain adalah membuat catatan transaksi publik secara cepat, murah dan aman dan ini menjanjikan potensi untuk dimanfaatkan bidang lain di luar sektor keuangan. Sebagai contoh misalnya untuk proses pemungutan suara dalam pemilihan umum atau pembuktian bahwa sebuah catatan (dokumen) benar-benar telah dibuat pada waktu tertentu. Blockchain juga sangat cocok digunakan untuk kondisi di mana diperlukan untuk mengetahui sejarah kepemilikan suatu barang seperti tanah, properti dan lainnya. Potensi blockchain untuk mengelola *supply chain* secara lebih baik juga sangat menjanjikan karena bisa memberikan kepastian terkait asal-usul barang tambang atau hasil hutan benar-benar dihasilkan dari proses-proses secara etis misalnya tidak melanggar hak asasi manusia atau eksploitasi hutan secara tidak bertanggung jawab.

Yang lebih menarik dalam laporan tersebut EPRS juga meyakini bahwa blockchain memiliki potensi untuk merevolusi berbagai lini bisnis dan kehidupan. Dengan kekuatan utamanya menggeser kontrol *ledger* (buku besar) yang berisi catatan transaksi menjadi terdesentralisasi dan bisa dilakukan oleh semua penggunanya menjadikan sistem ini lebih transparan dan, mungkin juga lebih demokratis. Apalagi melihat kecenderungan yang ada saat ini, dimana banyak pemerintahan di berbagai negara maupun industri yang telah dan terus melalukan penelitian blockchain arahnya juga ke sana. Mereka tidak mencoba untuk menegasikan berbagai keunggulan dan manfaat blockhain, justru ingin memanfaatkannya demi perbaikan layanan terhadap pelanggan maupun publik.

Dalam laporan tersebut, EPRS juga menyorot pentingnya dilakukan kajian lengkap dalam pengimplementasian blockchain. Hal ini dikarenakan selain banyaknya manfaat yang ditawarkan, teknologi blockchain juga menghadirkan sejumlah kerentanan baik dari sisi teknologinya sendiri maupun berbagai dampak yang akan muncul dengan pengimplementasiannya. Sebagai contoh misalnya, transparansi yang ditawarkan blockchain akan menjadi nilai tambah jika hal tersebut diterapkan untuk 'pencatatan' soal kepemilikan lahan. Namun bagaimana jika hal diterapkan untuk saldo tabungan dan data personal lainnya. Persoalan privasi dan anonimitas akan muncul di sana dan transparansi justru akan membahayakan. Faktanya, beberapa aplikasi blockchain yang telah dikembangkan tidak menawarkan anonimitas penuh, padahal sejumlah informasi sensitif tidak boleh 'didistribusikan' dengan cara itu. Karena itu menurut EPRS penting untuk mempersiapkan berbagai langkah antisipatif untuk meminimalkan dampak negatif pengimplementasiannya.

Dari berbagai potensi, dampak dan langkah antisipatif yang dilaporkan EPRS, kami sajikan beberapa yang mungkin tidak terlalu lama lagi bakal menjadi trend, termasuk di Indonesia.

Konten Digital: Blockchain dan Rights Management



Pemalsuan dan penipuan karya seni telah terjadi sejak lama. Namun di era Internet, hal tersebut bisa dilakukan dengan lebih mudah. Konten media telah banyak disalin dan dibagikan - seringkali secara ilegal – berkat sistem hi-fi di setiap rumah yang memudahkan untuk menyalin rekaman dan siaran radio ke kaset. Dan Internet membuat pembajakan menjadi lebih mudah. Ditahap awal hal tersebut diorganisir jaringan global untuk membagikan salinan CD melalui pos. Ketika e-format muncul ditambah ketersediaan bandwidth yang semakin meningkat, jaringan file sharing menjadikan pembajakan makin merajalela. Saat ini, pembajakan media paling sering diatur melalui 'torrents' dan, semakin meningkat dengan, streaming.

Meskipun distribusi konten media dengan cara ini seringkali ilegal, praktiknya begitu meluas dan penegakan hukum untuk mengatasinya begitu sulit diterapkan. Baru-baru ini, dengan melegitimasi layanan berlangganan, telah menggantikan beberapa pembajakan dengan menyediakan akses ke media dengan membayar royalti kepada pemegang hak cipta dengan menggunakan pendapatan dari biaya keanggotaan atau iklan. Meski begitu tidak ada model distribusi yang berhasil menjawab tantangan perdagangan konten digital di era Internet secara efektif - sampai mungkin teknologi blockchain muncul, sehingga bisa sedikit menyeimbangkan kepentingan antara pencipta, pelanggan, dan berbagai perantara.

Ketika konsumen membeli buku dan cakram, mereka datang untuk memiliki artefak/bentuk fisik yang nantinya dapat mereka jual-belikan dan dipindah kepada pihak lain. Meski begitu ada batasan atas hak mereka yang memiliki buku atau cakram tersebut, misalnya mereka tidak boleh mendistribusikan salinan, dan harus membayar royalti jika mereka menyiarkan konten. Dalam pembelian konten digital lainnya yang tidak memiliki bentuk fisik, konsumen tahu bahwa mereka tidak akan mendapatkan kepemilikan artefak fisik, tetapi banyak dari mereka yang tidak menyadari bahwa mereka juga tidak mendapatkan kepemilikan konten digital yang mereka 'beli'. Sebaliknya, mereka menandatangani perjanjian untuk lisensi yang berlaku untuk jangka waktu tertentu atau berapa kali mereka bisa memainkannya. Lisensi ini tidak dapat dijual, diberikan atau bahkan ditinggalkan sebagai bagian dari warisan. Mengoleksi musik, literatur, game, dan film digital yang dimiliki secara sah seringkali membutuhkan biaya yang sama dengan mengkoleksi berbagai cakram dan buku dengan konten yang sama. Ini adalah investasi seumur hidup yang besar tetapi tidak dapat dijual belikan.

Pertanyaannya mungkinkan teknologi blockchain membantu mengatasi masalah tersebut dan persoalan lain dari media digital ini?

Bagaimana Digital Rights Bisa Dikelola Dengan Blockchain

Teknologi Blockchain dapat digunakan untuk mengelola hak-hak konsumen atas produk-produk digital. Dalam banyak kasus, hal ini akan terkait dengan produksi ulang karya digital secara masal, termasuk disana CD, DVD dan buku, di mana pencipta karya seni tersebut menjual salinan dari karyanya dalam jumlah besar. Hal ini juga relevan untuk bentuk karya digital lain yang lebih unik, seperti lukisan misalnya. Dalam konteks ini pembeli tidak membeli versi salinan, seperti MP3 untuk lagu, melainkan hak eksklusif atas karya asli itu sendiri. Blockchain dapat melindungi konsumen dan pencipta karya digital dari segala jenis pembajakan dengan merekam sejarah kepemilikan produk digital dan bahkan mungkin sekaligus digital rights-nya itu sendiri.

Blockchain dapat digunakan untuk mencatatkan semua transaksi penjualan, pinjaman, donasi dan pemindahan tanganan CD, DVD dan bentuk-bentuk fisik lainnya yang memuat konten digital dari setiap individu. Semua transaksi yang terjadi akan 'disaksikan' dan 'disetujui' oleh semua pihak yang terlibat. Hal ini tidak berbeda

dengan transaksi dalam rekening bank atau pendaftaran kepemilikan tanah, yang tidak dapat dipindahtangankan kecuali oleh pemiliknya yang sah sesuai aturan. Disamping itu pembeli juga dapat dengan mudah melakukan verifikasi atas sah atau tidaknya salinan file MP3 atau video yang mereka beli. Dengan demikian seluruh transaksi tersebut bisa diverifikasi sehingga pembeli dapat menelusurinya hingga ke penciptanya.

Konsep ini dapat dikombinasikan dengan *smart contract* yang memungkinkan akses ke konten tersebut dapat dipindahkan kepada orang lain untuk periode yang tertentu sebelum dikembalikan secara otomatis dan ini dapat di-setting dimuka sampai periode berakhirnya 'ijin' akses terhadap konten tersebut. Agar semua ini berfungsi, sangat penting untuk diketahui bahwa ketika kepemilikan konten dipindahkan dari satu pihak ke pihak lain, pemilik sebelumnya telah kehilangan haknya akses, seperti yang terjadi jika mereka menjual piringan hitam di pasar barang bekas. Informasi terkait tentang kapan pengguna dan berakhirnya sama penting dengan dengan mengetahui kapan hak pengguna lain dimulai.

Di sinilah, blockchain dapat berperan. Dengan blockchain memungkinkan pelanggan untuk memastikan bahwa mereka membeli barang yang sah dan disaat bersamaan memungkinkan pemegangnya mengetahui hak-haknya. Untuk memverifikasi kepemilikan yang sah bahkan juga dapat dilakukan melalui teknologi, meskipun hal tersebut masih membutuhkan pengembangan codecs, standar industri, dan format file baru yang mem-*bundle* konten tu sendiri dengan izinnya.

Selain membeli salinan karya digital berlisensi seperti lagu MP3, juga mungkin untuk membeli dan menjual karya aslinya, yaitu lagu itu sendiri. Sama seperti membeli lukisan asli akan lebih banyak memiliki hak daripada hanya membeli salinan lukisan tersebut, seperti pembeli karya digital asli juga membeli hak eksklusif untuk menyiarkan konten, untuk menjual salinannya, dan untuk mengambil tindakan terhadap orang lain yang menggunakan konten secara tidak sah. Bagi pembeli, sangat penting untuk mengetahui apakah mereka membeli kepemilikan dari karya itu sendiri dengan nilai dan hak yang terkait, atau hanya reproduksi yang dilisensikan untuk penggunaan pribadi. Dalam hal ini, blockchain dapat digunakan untuk memverifikasi pemilik konten yang sebenarnya, apakah itu versi asli atau salinan sahnya, dan kumpulan hak yang di-*bundle* dengan konten tersebut.

Selain dari hak penjual dan pembeli, blockchain juga dapat digunakan untuk melindungi hak cipta dari pembuat karya yang asli, sehingga memiliki kepastian akan beberapa hak setelah menjual karyanya tersebut. Pengertian pembuat asli di sini bisa terdiri dari sejumlah pelaku yang kompleks dan masing-masing memiliki hak atas pembayaran royalti ketika konten tersebut digunakan untuk tujuan komersial. Untuk trek musik, misalnya, jaringan kreator tersebut bisa terdiri dari penulis, musisi, dan artis lain serta manajer, dan lainnya. Hak masing-masing aktor ini, serta syarat dan cara penggantian mereka dapat dikodekan secara digital, memungkinkan pembayaran yang lebih andal dan efisien. Pembayaran royalti bahkan bisa dilaksanakan secara otomatis melalui *smart contract*.

Potensi Pengembangan dan Dampaknya

Penggunaan teknologi blockchain dengan cara ini bisa menjadi yang pertama kalinya dan memungkinkan konsumen untuk membeli dan menjual salinan digital ke tangan kedua, memberikan mereka atau menyumbangkannya sebagai amal, meminjamkannya kepada teman-teman untuk sementara atau meninggalkan mereka sebagai bagian dari warisan - dengan jaminan mereka tidak menyebarkan salinan digital yang tidak berlisensi. Agar blockchain bisa mendukung metode pengelolaan hak digital yang belum bisa dilakukan metode lainnya, menuntut penyeimbangan hak penjual, pembeli, jaringan kreator lainnya, termasuk yang mengembangkan dan memelihara blockchain itu sendiri. Dengan jaringan kepentingan yang rumit seperti itu, menjadi lebih ideal untuk mengharapkan solusi yang cepat dan tidak memunculkan kontroversi.

Kebijakan Antisipatif

Hukum akan terus memiliki peran penting dalam mengidentifikasi karya cipta dan menyelesaikan sengketa. Pengembangan Blockchain di bidang ini dapat mengarah pada kebijakan perizinan multi-teritorial dan meningkatkan kepastian hukum bagi para kreator dan pembeli paralel dengan menyediakan mekanisme penyelesaian sengketa yang efektif, khususnya dalam kaitannya dengan tarif, ketentuan perizinan, pengesahan hak online untuk pengelolaan dan penarikan hak secara *online*.



Paten: Melindungi Inovator dan Memberikan Insentif pada Inovasi

Paten memberi pemiliknya hak eksklusif untuk memanfaatkan hasil inovasinya untuk periode tertentu. Sistem paten memang dirancang untuk memberikan insentif bagi inovasi berupa kesempatan bagi inovator untuk mendapatkan keuntungan dari ide dan kreasi yang mereka lakukan. Namun melindungi inovator berbeda dengan mendorong inovasi. Sistem paten harus menyeimbangkan perlindungan terhadap inovator maupun para kompetitor. Jika inovator tidak dilindungi, maka kompetisi yang bebas akan menghambat lahirnya inovasi-inovasi baru. Sebaliknya, jika kompetitor tidak dilindungi, mereka tidak akan mau melakukan investasi untuk mendorong peningkatan dan penghematan biaya dengan memanfaatkan hasil inovasi tersebut.

Pada dasarnya, sistem paten dapat dilihat sebagai sistem pertukaran yang diberikan pemerintah kepada inovator untuk memonopoli (terbatas dalam waktu dan ruang lingkup) serta mengeksploitasi inovasi mereka dan mendapatkan keuntungan dari sana. Sebagai gantinya pemegang paten harus mempublikasikan secara rinci bagaimana inovasi mereka bekerja dan membantu mengembangkan berbagai perbaikan atau menciptakan cara-cara baru sebagai alternatif untuk orang lain.

Namun sejumlah persoalan muncul terkait sistem paten. Misalnya, pesaing terkadang dapat mengeksploitasi paten sebelum inovator, baik karena paten tidak cukup kuat atau karena pemegang paten tidak mampu membela diri terhadap pelanggaran paten yang terjadi. Belum lagi ditambah persoalan biaya yang harus dikeluarkan untuk mendapatkan perlindungan paten tersebut sementara sistem paten seringkali berbeda-beda di sejumlah negara dan belum menggunakan standar yang sama. Akibatnya tidak sedikit perusahaan yang lebih suka mengambil risiko dengan membawa inovasi mereka ke pasar tanpa perlindungan paten sama sekali.

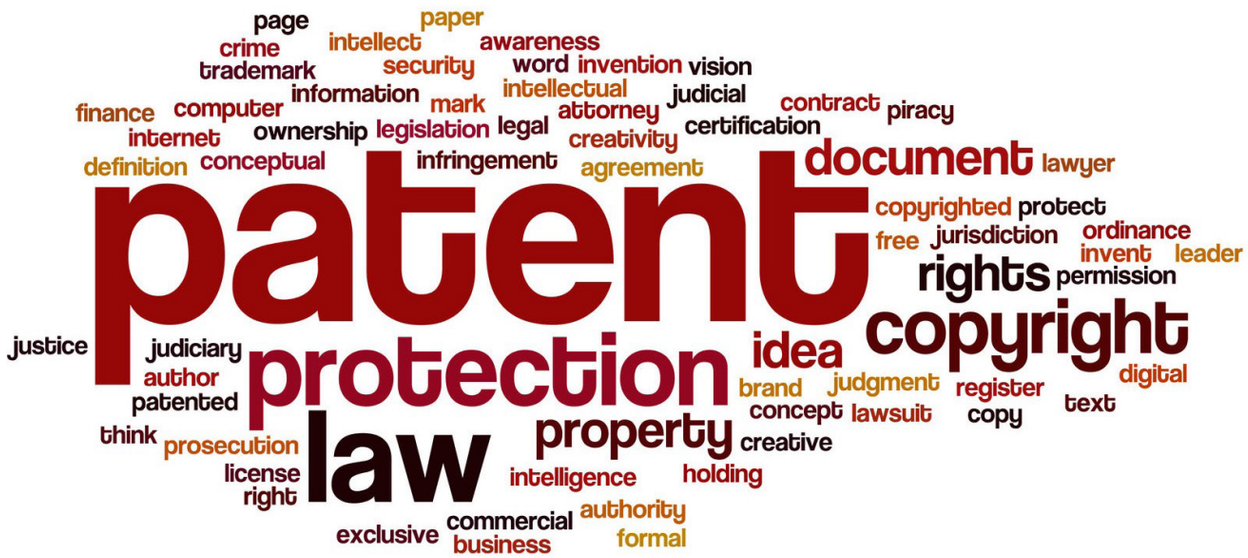
Kompleksitas sistem paten juga menghadirkan persoalan lain. Di negeri kita bahkan ditambah dengan masih minimnya kesadaran akan pentingnya paten tersebut menjadikan tidak sedikit inovator yang malas mengajukannya. Di benak para inovator mendaftarkan paten cukup merepotkan dan membutuhkan biaya yang tidak sedikit.

Masalah lebih lanjut untuk sistem paten yang teridentifikasi adalah munculnya *'troll patent'*, yakni paten bisa dimiliki oleh orang/pihak yang tidak melakukan inovasi. Meskipun klaim mereka tidak selalu memiliki dasar hukum yang kuat, perusahaan/inovator seringkali tidak mampu atau tidak mau menanggung biaya hukum yang diperlukan untuk memperjuangkannya dan lebih memilih penyelesaian di luar sistem peradilan yang berlaku.

Di sisi lain saat ini sudah semakin banyak aspek dari sistem paten yang telah didigitalkan, namun tidak ada perubahan besar pada strukturnya sejak revolusi informasi.

Bagaimana blockchain dapat membantu sistem paten?

Teknologi blockchain memiliki dua fitur yang sangat relevan dengan sistem paten, yakni *'hashing'* dan *'proof of existence'* atau sering juga di sebut *'proof of work'/*



mining. Setiap data digital memiliki identitas digital yang disebut 'hash'. Proses di mana setiap data/dokumen diubah menjadi kode-kode digital dikenal sebagai 'hashing' Setiap hash itu unik. Perbedaan yang sangat kecil, seperti hilangnya salah satu huruf pada sebuah 'nama' dokumen/ data, akan mengarah pada *hash* yang sangat berbeda. Satu-satunya cara untuk menghasilkan hash yang sama adalah mengulangi *hashing* itu sendiri. Jadi sangat kecil kemungkinan mengganti sebuah dokumen dari *hash*-nya tersebut.

Sementara fitur *'proof of existence'* (*POE*) merupakan proses validasi data yang dibuat sehingga bisa meminimalisir pemalsuan data. Dengan proses tersebut akan diketahui waktu pembuatan *hash*. POE bisa dilakukan oleh setiap orang melalui komputer yang terhubung di jaringan blockchain, tetapi tidak dapat melihat isi data tersebut. Dengan demikian kecuali pembuat data transaksi tidak akan bisa mengubah atau menyalin data tersebut.

Keunggulan ini menyajikan peluang yang menarik untuk mencatat setiap transaksi yang dilakukan tanpa kekhawatiran isi dokumen transaksi itu diketahui publik. Para inovator dapat memanfaatkan fitur tersebut untuk membuat catatan hasil inovasi mereka pada blockchain tanpa kekhawatiran diketahui atau 'diakses' secara ilegal oleh para kompetitor.

Penerapan teknologi blockchain dalam sistem paten dapat mengurangi ketidakefisienan dalam pengodean ulang dan waktu pendaftaran paten dengan cara yang lebih efisien. Fitur POE memungkinkan layanan berbasis blockchain diterapkan pada tahap awal dengan demikian juga bisa memastikan keamanan sekaligus kemudahan dan transparansi bagi pemohon dalam setiap tahapan proses pendaftaran paten secara keseluruhan-termasuk menutup pintu terjadinya praktik-praktif korupsi dalam pengurusan paten.

Kebijakan Antisipatif

Sistem paten yang berlaku saat ini dapat disederhanakan dengan penggunaan teknologi blockchain. Selain itu lembaga resmi yang mengurusi persoalan paten ini dapat menyediakan layanan yang lebih murah melalui layanan yang mengoptimalkan fitur POE pada teknologi blockchain. Meski begitu perlu ditekankan bahwa POE berbasis blockchain tidak serta-merta identik dengan proteksi paten itu sendiri. Seperti halnya layanan POE pada Bitcoin yang disediakan pihak ketiga, dan diterima untuk melegitimasi catatan transaksi, lembaga yang berwenang dalam pengurusan paten ini terlebih dahulu harus mengakui dan melegalisasi pemanfaatan POE tersebut.





E-voting: Revolusi Sistem Elektoral

Meski digitalisasi telah merasuk ke berbagai aspek kehidupan modern saat ini, namun penyelenggaraan pemilu di banyak negara masih mempertahankan cara-cara tradisional berbasis kertas. Sejak beberapa tahun lalu, e-voting dianggap menjadi salah satu inovasi yang menjanjikan untuk mempercepat, menyederhanakan dan mengurangi biaya pemilihan umum. Meski begitu, banyak ahli yang merasa skeptis terhadap penggunaan e-voting untuk pemilihan umum tingkat nasional, dengan alasan kesiapan dukungan sistem keamanan yang mumpuni belum tersedia. Namun mereka meyakini penggunaan e-voting berbasis teknologi blockchain sudah dapat diterapkan untuk pemilihan umum tingkat daerah-pilkada.

Bagaimana blockchain dapat digunakan untuk *e-voting*?

Blockchain merupakan suatu cara *logging* dan verifikasi setiap catatan secara transparan dan terdistribusi pada semua *user*. Sementara vote (suara) dalam sebuah pemilu biasanya tercatat, dikelola, dihitung dan di verifikasi oleh sebuah lembaga yang diberikan otoritas untuk itu- Komisi Pemilihan Umum. *e-voting* yang didukung teknologi blockchain (BEV) memungkinkankan para pemilih untuk melakukan tugas lembaga tersebut. Dengan demikian kemungkinan manipulasi suara bisa sangat diminimalisir. Suara tidak sah misalnya tidak akan bisa dihitung, karena para pemilih juga tahu aturan yang telah ditetapkan. BEV bisa dimanfaatkan sebagai pengganti lembaga pengawas pemilu atau saksi-saksi dengan berbasiskan teknologi.

Salah satu cara mengembangkan sistem BEV adalah dengan membuat sebuah sistem baru yang dirancang sesuai dengan karakteristik sistem pemilu yang digunakan. Cara lain yang lebih mudah dan murah bisa adalah dengan memanfaatkan aplikasi teknologi blockchain yang sudah mapan seperti Bitcoin. Mengingat bahwa keamanan buku besar (*ledger*) blockchain sangat bergantung pada luas basis penggunanya, maka cara ini kemungkinan besar juga menawarkan keamanan yang lebih baik untuk pemilihan dengan skala yang lebih kecil-jumlah pemilihnya lebih sedikit dan juga dari sisi biaya menjadi lebih ekonomis dibandingkan jika mengembangkan sistem baru berbasis blockchain.

Potensi pemanfaatan BEV dalam konteks organisasi memang sangat besar. Sebagai contoh, di Denmark, BEV telah dimanfaatkan dalam pemilihan internal sebuah partai politik, sementara di Estonia digunakan untuk mengetahui suara dan keinginan seluruh pemegang saham sebuah perusahaan. Bahkan dalam konsep yang lebih maju, BEV dapat dikombinasikan dengan *smart contract*, untuk secara otomatis mengambil tindakan pada kondisi tertentu yang telah disepakati bersama. Sebagai contoh terkait hasil pemilu misalnya, adalah untuk memastikan janji-janji pemenang pemilu direalisasikan, pilihan investasi dalam sebuah perusahaan atau keputusan organisasi lainnya.

Potensi Pengembangan dan Dampak

Melihat penerapannya dalam pemilihan kepala daerah dan pengambilan pengambilan keputusan organisasi, BEV dapat membantu meningkatkan partisipasi publik secara *bottom up* dengan menawarkan sistem *e-voting* yang relatif murah dan aman. Memang masih muncul kekhawatiran



terkait anonimitas dan aksesibilitas yang ditawarkan oleh BEV, Namun, sejatinya kekhawatiran tersebut juga menjadi perhatian pada sistem pemilu tradisional yang ada saat ini.

Soal krusial lainnya adalah bagaimana menjamin keamanan dan legitimasi sistem tersebut sehingga dapat dipercaya secara lebih luas. Seperti halnya pemilu berbasis kertas, hasilnya tidak cukup adil dan valid. Semua pemilih, bahkan jika mereka kecewa dengan hasilnya, harus menerima bahwa keseluruhan proses itu sah. Dengan demikian, selain memberikan keamanan dan akurasi, BEV juga harus bisa mendapatkan kepercayaan secara luas. Memang harus diakui bahwa faktanya protokol blockchain ini cukup rumit yang kemungkinan besar menjadi kendala diterimanya sistem ini secara luas.

Potensi BEV yang tidak hanya mendigitalkan proses pemungutan suara tradisional, melainkan juga menawarkan alternatif dengan serangkaian nilai dan pondasi politik yang berbeda. Secara tradisional, otoritas pemilu mengelola pemilihan dan prosesnya terpusat dan *top-down*. BEV adalah kebalikannya. Proses ini dikelola oleh masyarakat dan transparan, terdesentralisasi dan *bottom-up*. Sementara partisipasi dalam pemilihan tradisional memperkuat otoritas negara, partisipasi dalam BEV menegaskan kuasa masyarakat. Dalam konteks inilah sangat jelas hubungan antara BEV dan transisi menuju demokrasi langsung, terdesentralisasi dan *bottom-up* dengan demokrasi itu sendiri. Meski demikian, sejauh mana teknologi blockchain akan berkembang di bidang *e-voting* sangat tergantung bagaimana e-voting mampu merefleksikan nilai-nilai dan struktur masyarakat, politik dan demokrasi di sebuah negara.

Kebijakan Antisipatif

Meskipun organisasi secara luas bisa bebas untuk mengatur pemilihan internal dengan memanfaatkan blockchain, tetap saja harus mematuhi regulasi-regulasi yang berlaku. Di Eropa misalnya pemanfaatan BEV ini tetap harus mematuhi peraturan tentang privasi dan perlindungan data. Meskipun secara protokol pemilihan umum di negara-negara Uni Eropa tidak di atur namun beberapa konvergensi telah terjadi dan upaya untuk mendorong penggunaan *e-voting* terus dilakukan dengan tetap menghormati prinsip-prinsip konstitusi hukum pemilu (universal, sama, gratis, rahasia dan langsung-atau di Indonesia kita kenal langsung, umum, bebas, dan rahasia).



Smart Contracts: Ketika Kode Menjadi Hukum

Dibandingkan dengan centralized ledgers yang ada saat ini, sejumlah fitur baru dan canggih disediakan ledgers (buku besar) berbasis teknologi blockchain. Selain mendokumentasikan waktu pembuatan dan rincian transaksi, teknologi blockchain juga memungkinkan pencatatan transaksi tersebut diatur sekaligus untuk mengeksekusinya secara otomatis dengan cara menanamkan kode untuk merespon berbagai kondisi yang telah disepakati.

Fitur yang kemudian dikenal sebagai *self-executing smart contracts* saat ini mulai berkembang pesat. Pertanyaan yang kemudian muncul adalah bagaimana ketika kode dan hukum menjadi satu.

Cara Kerja

Meski pengertian *smart contracts* bisa merujuk pada beberapa beberapa konsep yang berbeda, berdasarkan definisi tahun1994 adalah 'protokol transaksi terkomputerisasi yang mengeksekusi ketentuan-ketentuan perjanjian', tetap sangat relevan digunakan dalam konteks teknologi blockchain. Dengan bahasa yang lebih sederhana adalah ketentuan perjanjian antara dua pihak atau lebih diprogram ke dalam kode (seperangkat instruksi) yang disimpan di blockchain dengan cara yang sama seperti transaksi yang secara rutin disimpan pada blockchain lainnya.

Ketika kondisi tertentu yang dijelaskan dalam kode terpenuhi, otomatis akan memicu tindakan spesifik, yang juga didefinisikan dalam kode, Jadi, misalnya, pengiriman produk bisa memicu instruksi untuk melakukan pembayaran. Hal ini pada gilirannya akan memicu instruksi lain dalam *smart contracts* lainnya, seperti misalnya mungkin untuk menukarkan mata uang atau membuat pemesanan selanjutnya ke rantai pasokan. Banyak contoh aplikasi *smart contracs* lainnya, khususnya di sektor keuangan seperti untuk produk-produk pinjaman dan asuransi produk asuransi untuk mengotomatisasi proses-prosesnya yang selama ini masih dilakukan secara manual. Di luar dunia keuangan, aplikasi *smart contracts* juga bisa digunakan untuk mengotomatisasi pemberian hak waris hingga konten digital.

Salah satu platform berbasis blockchain, yakni Ethereum memiliki fitur bahasa pemrograman dan mata uang sendiri, yang dibuat khusus untuk mendukung *smart contracts*. Pendekatan untuk *smart contract* juga digunakan pada implementasi blockchain yang lain termasuk Bitcoin.

Saat ini implementasi *smart contracts* memang lebih cocok diterapkan untuk perjanjian-perjanjian yang lebih bersifat jangka pendek. Sementara untuk kontrak jangka panjang masih menemui sejumlah kendala. Diantara berbagai kendala tersebut yang paling signifikan adalah penerapan *smart contracs* membutuhkan biaya yang tidak sedikit dan kebutuhan akan pengaturan *smart contracs* di awal sebelum 'dimasukkan di jaringan blockchain. Kedua persoalan ini memang masih menyisakan tantangan, sebab kesepakan yang telah dibuat diatas platform blockchain menjadikannya tidak mudah diubah selama periode perjanjian. Padahal faktanya adanya ketidakpastian hukum yang harus menjadi pertimbangan. Dengan kata lain saat ini pembuatan *smart contracts harus* benar-benar bisa mencerminkan konsensus dan kesepakatan kedua belah pihak sehingga kemungkinan terjadinya *dispute* di masa yang akan datang dapat diminimalisir.

Hak lain, yang harus diingat adalah *smart contract*s sangat dipengaruhi oleh stimulus digital yang kemudian memicu proses-proses digital selanjutnya. Karena itu akan menjadi lebih efektif jika berbagai klausul dan konsekuensinya juga menghitung aspek aspek lingkungan digital. Dengan demikian *smart contract* benar-benar cocok untuk mengotomatisasi berbagai proses-proses yang selama ini masih dilakukan secara tradisional.

Potensi dan Dampaknya

Sebagaimana diketahui catatan transaksi di dalam buku besar berbasis blockchain tidak mudah diubah dan kode maupun kontraknya hanya dapat dibatalkan atau dimodifikasi berdasarkan persyaratan yang telah diizinkan dalam kode itu sendiri. Hal ini berbanding terbalik dengan perjanjian-perjanjian yang dibuat secara konvensional yang memungkinkan salah satu pihak untuk mengubah dan atau melanggar, tentu saja dengan kesiapan untuk menanggung konsekuensinya sesuai dengan kesepakatan yang dibuat. Dengan *smart contract*s hal demikian sudah tidak dimungkinkan lagi, karena semua transaksi sudah diotomatisasi.

Dengan alasan itulah jika kemudian muncul interpretasi bahwa *smart contracts* akan menjadikan kode-kode itu sebagai hukum - *self contained*, *self performed* dan *self-enforced*. Dan ini membuat tidak sedikit kalangan yang memposisikan *smart contracts* diluar kendali struktur yang sudah mapan, seperti negara dan yurisdiksi hukum. Dengan menganggap kode sebagai hukum, kesalahan atau kerentanan yang tidak disengaja menjadi bagian dari perjanjian itu sendiri. Mengeksploitasi *bug* dalam konteks ini untuk mengendalikan aset tidak akan dianggap lagi sebagai pencurian, karena kesalahan yang memungkinkan penarikan adalah bagian dari kode dan dengan demikian, tidak menyalahi definisi, dalam 'hukum'.

Di sisi lain tak sedikit pula pihak yang menempatkan *smart contract* sebagai bagian sistem hukum yang lebih luas. Sama halnya dengan perjanjian konvensional, persyaratan tambahan dapat dikenakan, dan klausul dapat dibatalkan atau ditafsirkan ulang atas dasar kesepakatan para pihak dan hukum yang lebih luas. Hukum negara selalu berada di atas 'hukum' yang tertulis dalam kode, meskipun proses hukum dan penegakannya terbukti sulit.

Tidak seperti penerapan blockchain secara sederhana yang mencatat transaksi, *smart contract* mencakup kode-kode yang dapat dieksekusi sehingga menghadirkan kompleksitas yang lebih. Hal ini juga berarti penerapan *smart contracts* membutuhkan sistem yang memiliki kemampuan untuk melakukan pemrrosesan yang lebih baik dan tentu saja perawatan sistem itu sendiri yang jelas membutuhkan biaya yang lebih mahal termasuk untuk biaya listrik. Selain itu kompleksitas sistem juga memunculkan berbagai kerentanan dari sisi keamanan, plus interpretasi *code as law* menjadikan *smart contracs* tidak mudah di dalam penerapannya.

Kebijakan Antisipatif

Tidak sedikit bidang hukum yang sangat rentan terhadap eksploitasi di mana perjanjian tidak dianggap sebagai bagian dari yurisdiksi hukum tradisional. Sebagai contoh adalah hukum perpajakan (misalnya terkait pendapatan, penjualan, warisan dan keuntungan modal), eksploitasi (misalnya kontrak sewa dan pekerjaan) dan kejahatan korporasi (mis. penetapan harga dan *insider trading*). Karena itu sangat diperlukan cara-cara baru untuk menegaskan keutamaan hukum nasional jika otomatisasi yang ditawarkan smart contracts lebih sulit dalam penegakan hukumnya. Pemerintah memiliki tanggung jawab baru dalam proses penerapan proses peradilan tradisional untuk *smart contracts*, seperti *arbitrase* ketika *bug* ditemukan dalam kode perjanjian. Ketika programmer mulai menerjemahkan perjanjian ke dalam kode yang dapat dieksekusi, mereka secara efektif membuat keputusan tentang bagaimana mereka akan diimplementasikan dalam praktik, yang dapat berarti mereka membawa tanggung jawab hukum yang lebih besar.

Smart contracts bisa menjadi tidak fleksibel dan tidak dapat beradaptasi dengan perubahan keadaan atau preferensi kedua belah pihak yang melakukan perjanjian. Tidak semua pertanyaan mungkin dapat dijawab sebelumnya, dan akan selalu ada keadaan yang tak terduga yang memerlukan interpretasi tentang bagaimana klausul perjanjian harus diterapkan. Putusan sengketa kontrak dan penegakan klausa kontrak dapat menimbulkan tantangan seiring dengan berkembangnya bidang tersebut.

Hukum perjanjian konvensional, khususnya terkait berbagai persyaratan penyimpanan catatan transaksi dan aturan pembuktian, mungkin perlu dimodifikasi dengan memperhitungkan *smart contracts* yang bersifat otomatis dan deterministik, serta masalah yang berkaitan dengan validitas dan perberlakuannya. Undang-undang diharapkan dapat menjawab pertanyaan mengenai perlunya membangun hubungan secara fisik, melakukan prosedur validasi yang diperlukan dan memastikan kepatuhan aplikasi blockchain dengan hukum yang berlaku. Apakah kode-kode yang bersifat teknis bisa menjadi bentuk hukum yang paling signifikan? Kriteria jelas diperlukan untuk memastikan validitas hukum dan keberlakuan *smart contracts* di bawah aturan yang berlaku.



Supply chains: Tingkatkan Transparansi dan Akuntabilitas

Barang diproduksi dan didistribusikan melalui jaringan mulai produsen, distributor, pengecer, transportasi dan pemasok dalam sebuah proses pengelolaan perjanjian, pembayaran, pelabelan, penyegelan, logistik, anti-pemalsuan dan anti-penipuan yang sangat kompleks.

Skala dan kompleksitas *supply chain* (rantai pasokan) ini mendorong biaya transaksional yang tinggi, Ketidaksesuaian dan kesalahan sering terjadi dalam berbagai dokumen berbasis kertas. Pun sejumlah kerugian yang sering kali dipicu oleh berbagai faktor termasuk pencurian. Berbagai isu lain seperti; kerusakan lingkungan hingga imbasnya bagi kesehatan manusia pun sringkali disorot dunia terutama ketika persoalan tersebut memberikan dampak besar bagi masyarakat seperti kasus ilegal logging hingga tumpahnya minyak mentah di lepas pantai yang seringkali sebagai akibat rantai pasokan yang pengelolaannya kurang profesional.

Mungkinkah teknologi blockchain dapat diimplementasikan pada rantai pasokan ini, termasuk bidang logistik untuk meningkatkan efesiensi kegiatan operasional, memangkas kejahatan-penipuan dan pemalsuan barang serta sejumlah tantangan besar lainnya seperti eksploitasi tenaga kerja yang tidak etis dan degradasi lingkungan?

Bagaimana Rantai Pasokan Bisa Dikelola Dengan Blockchain

Aplikasi berbasis blockchain memiliki potensi untuk mengoptimalkan rantai pasokan dengan menyediakan infrastruktur untuk registrasi, sertifikasi dan pelacakan pada barang dengan biaya yang lebih rendah dan bisa ditransfer antar berbagai pihak yang sering terpisah jauh secara geografis. Keunikan setiap barang diidentifikasi melalui 'token' dan kemudian dapat ditransfer melalui blockchain. Setiap transaksi akan diverifikasi dan diberi tanda terkait waktunya dalam proses yang terenkripsi tetapi transparan.

Berbagai keunggulan yang ditawarkan teknologi blockchain tersebut memungkinkan pihak-pihak mulai dari pemasok, vendor, transporter atau pembeli bisa mengaksesnya. Meski begitu mereka tidak dapat membatalkan dan mengubah, walaupun setiap transaksi yang telah dibuat terbuka untuk diperiksa semua orang atau auditor yang telah diberi wewenang. Smart contract juga dapat digunakan untuk mengeksekusi pembayaran maupun prosedur lainnya secara otomatis.

Potensi dan Dampak

Sejumlah perusahaan, baik startup maupun '*big player*' telah menguji coba pemanfaatan blockchain untuk mendokumentasikan catatan transaksi dalam rantai pasokan mereka. Sebagai contohnya adalah aplikasi Everledger yang memungkinkan perusahaan dan pembeli untuk melacak asal usul berlian mulai dari tambang hingga dijual di toko-toko perhiasan untuk memankas kemungkinan fraud untuk asuransi atau dokumentasi. Untuk masing-masing berlian, Everledger menetapkan 40 atribut pengukuran mulai dari proses pemotongan hingga tempat penambangannya. Everledger memberikan nomor seri untuk setiap berlian yang ditulis secara mikroskopis, dan kemudian mereka menambahkan ID digital ini ke blockchain.

Dengan demikian berlian menjadi jelas asal-usulnya, dan pada akhirnya akan memangkas kemungkinan terjadinya kasus penipuan. Disamping itu kejelasan asal usul berlian tersebut juga sangat mempermudah aparat terkait baik polisi hingga penyelidik asuransi untuk melacak permata-permata yang dicuri. Bagi konsumen ini juga sangat menguntungkan karena memiliki kepastian akan 'asal-usul' berlian yang benar-benar 'bersih'.

Contoh aplikasi lain untuk rantai pasokan dikembangkan oleh Provenance, yakni sebuah perusahaan yang berbasis di London, telah mengembangkan platform data *real-time* untuk mengumpulkan dan memverifikasi asal usul suatu aset dengan menetapkan *token* atau 'paspor digital' yang dapat dilacak di seluruh rantai pasokan hingga mencapai tujuannya. Ini bisa berguna untuk menghindari penipuan dalam penjualan barang dengan mengaitkannya dengan asal-usul barang.

Blockchain juga bisa digunakan untuk meminimalkan risiko dalam pembayaran, seperti yang dikembangkan oleh Skuchain dan Fluent. Kedua perusahaan tersebut menawarkan dukungan berbasis blockchain untuk pembiayaan dan pembayaran di dalam rantai pasokan. Proyek lain adalah pengembangan sistem untuk merampingkan proses dokumentasi secara manual, melalui pemanfaatan privat blockchain untuk berbagi informasi antara eksportir, importir dan bank. Wal-Mart, pengecer terbesar di dunia, menguji coba blockchain untuk *food safety*. Wal-Mart mengharapkan dengan pencatatan transaksi yang akurat dapat membantu melakukan identifikasi produk, pengiriman dan vendornya, sehingga jika ada kejadian yang tidak diinginkan, manajemen dapat melacak dengan cepat dari mana sumber makanan tersebut berasal. Catatan yang akurat juga dapat membuat rantai pasokan menjadi lebih efisien karena pengiriman makanan ke toko dilakukan lebih cepat sehingga bisa mengurangi kerugian karena pembusukan dan limbah bahan-bahan makanan tersebut.

Tak hanya yang telah disebutkan dalam artikel sebelumnya, sistem berbasis blockchain juga memiliki potensi untuk meningkatkan efisiensi proses pengadaan, logistik dan pembayaran, mengurangi pemrosesan manual dokumentasi impor / ekspor, memastikan kesesuaian dan pengiriman barang dan mencegah kerugian, dengan demikian bisa mengurangi biaya, meningkatkan keselamatan dan keamanan, serta meminimalkan penipuan. Sistem ini juga dapat menjadi sarana untuk memverifikasi keaslian, asal dan standarisasi barang dan jasa.

Meski demikian kehati-hatian tetap harus dilakukan. Kepercayaan antar pelaku yang ada di rantai pasokan sangat tergantung pada teknologi blockchain, yang bagaimanapun tidak sepenuhnya bebas dari kerentanan, termasuk kesalahan yang tidak disengaja dan serangan siber lainnya. Otomatisasi tidak akan menjamin terhapusnya *bug*, konflik kepentingan atau korupsi dalam rantai pasokan global yang kompleks secara menyeluruh.

Blockchain memungkinkan semua transaksi menjadi lebih transparan, tetapi tidak secara eksplisit terkait dengan individu atau organisasi di dunia nyata, melindungi identitas pihak-pihak yang ada dirantai pasokan tanpa mengorbankan integritas catatan transaksi. Pemeriksaan semua atribut barang dan pergerakannya dapat dipisahkan dari identitas lengkap pengguna, menyembunyikan data pribadi yang sensitif melebihi apa yang diperlukan untuk pencatatan. Namun, anonimitas ini tidak mutlak dan dimungkinkan untuk menghubungkan transaksi dengan pihak-pihak tertentu. Banyak pihak yang mengharapkan sistim ini bisa ditingkatkan karena masih bisa melanggar privasi, seperti misalnya Setelah barang diterima konsumen, fitur pelacakan secara detil harus otomatis terhenti, atau setidaknya diperbaiki untuk memenuhi standar privasi dan perlindungan data.

Kebijakan Antisipatif

Pengembangan blockchain dalam manajemen rantai pasokan menghadapi tantangan dari regulasi. Di sejumlah negara, khususnya di kawasan Eropa aturan yang mewajibkan pelaporan non finansial akan berdampak pada pengembangan aplikasi blockchain untuk rantai pasokan ini. Aturan tersebut mewajibkan organisasi atau perusahaan untuk mengungkapkan informasi yang dapat dipercaya tentang masalah lingkungan, aspek sosial dan karyawan, penghormatan terhadap hak asasi manusia, dan isu-isu anti korupsi, sehingga mendorong lebih banyak transparansi dalam operasi mereka.

Namun begitu, ketiadaan perantara di sebagian besar atau semua tahapan rantai pasokan berbasis blockchain ini di masa depan dapat menciptakan ketidakpastian bagi pihak-pihak yang terlibat, terutama ketika menyangkut bentuk-bentuk eksekusi dan pengawasan transaksi yang berjalan secara otomatis. Dalam kebanyakan kasus, gagasan dan mekanisme untuk pertanggungjawaban dan tanggung jawab ketika masalah yang tak terduga terjadi harus ada atau ditata ulang.



Blockchain States: Rethinking Public Services

Dalam konteks keterbukaan data, layanan, dan keputusan di sektor publik melalui teknologi digital, pengembangan dari layanan e-government next generation yang lebih terbuka, bertanggung jawab, transparan dan kolaboratif terus dilakukan di berbagai negara. Baru-baru ini Government Chief Scientific Advisor Inggris menerbitkan laporan yang menguraikan bagaimana teknologi berbasis blockchain dapat menjadi alat baru untuk mengurangi penipuan, menghindari kesalahan, memangkas biaya operasional, meningkatkan produktivitas, mendukung kepatuhan dan meningkatkan akuntabilitas di berbagai layanan publik. Aplikasi – aplikasi yang potensial termasuk untuk pengumpulan pajak, pengelolaan identitas, distribusi manfaat, mata uang digital lokal (atau nasional), properti dan pendaftaran tanah dan semua jenis catatan pemerintah. Teknologi yang sama juga membuka pintu bagi aktor non-negara untuk menyediakan layanan serupa negara, dari layanan notaris hingga kewarganegaraan global dan identitas.

Pertanyaannya apa teknologi blockchain ini akan memberikan manfaat lebih bagi peningkatan layanan publik? Ini masih harus terus dilihat mengingat baru dimulai.

Bagaimana teknologi blockchain Bisa Membantu Peningkatan Layanan Publik

Data yang digunakan oleh lembaga-lembaga publik seringkali terbagi-bagi dan tidak jelas antara warganegara, pebisnis atau pengawas. Teknologi blockchain memungkinkan perekaman data dibuat dan diverifikasi secara lebih cepat, aman, dan transparan. Pemanfaatan aplikasi teknologi blockchain yang bisa segera dilakukan dalam administrasi publik adalah pencatatan. Kombinasi pencatatan waktu (time-stamping) dengan tanda tangan digital pada buku besar yang mudah diakses diharapkan bisa memberikan manfaat bagi semua pengguna. Hal itu memungkinkan masyarakat untuk melakukan transaksi dan membuat catatan (misalnya untuk pendaftaran sertifikasi tanah, akte kelahiran dan izin usaha) dan mengurangi ketergantungan pada pengacara, notaris, pejabat pemerintah dan pihak ketiga lainnya.

Pemerintah Estonia telah melakukan eksperimen pengimplementasian blockchain yang memungkinkan warganegara untuk memesan resep obat, pemilihan umum, urusan dengan bank, mendaftarkan bisnis mereka, membayar pajak dan mengakses sekitar 3.000 layanan digital lainnya hanya dengan menggunakan kartu ID - KTP. Sebaliknya dengan penggunaan blockchain tersebut, aparat birokrasi melakukan enkripsi dokumen, menelaah dan menyetujui izin, kontrak dan aplikasi dan mengirimkan permintaan informasi ke layanan lain.

Apa yang dilakukan Pemerintah Estonia adalah contoh menarik penerapan blockchain untuk meningkatkan berbagai layanan publik dengan tetap membatasi akses berbagai data publik untuk melindungi data dan privasi pengguna. Ini juga menjadi contoh inisiatif pemanfaatan blockchain yang paling maju oleh lembaga pemerintahan.

Beberapa negara lain termasuk Ghana, Kenya, dan Nigeria telah mulai menggunakan blockchain untuk mengelola pendaftaran tanah. Tujuan mereka adalah untuk membuat catatan kepemilikan tanah yang jelas dan dapat dipercaya, untuk menjawab tantangan persoalan pendaftaran tanah, korupsi dan juga tingkat akses publik yang buruk terhadap dokumen pertanahan di negara-negara tersebut. Di Swedia juga sedang dilakukan ujicoba untuk menempatkan transaksi real estat di blockchain, yang memungkinkan semua pihak yang terlibat - bank, pemerintah, broker, pembeli dan penjual bisa melacak progres transaksi dalam semua tahapannya dan menjamin keaslian dan transparansi dari proses-proses tersebut serta untuk menghemat waktu dan biaya.

Departement for Work & Pensions di Inggris juga telah menguji coba penggunaan teknologi blockchain untuk

pembayaran tunjangan jaminan kesejahteraan sosial. Warga cukup menggunakan ponsel mereka untuk menerima dan menghabiskan pembayaran tunjangan mereka dan, dengan persetujuan mereka, transaksi mereka dicatat di dalam buku besar yang didistribusikan. Tujuan dari inisiatif ini adalah untuk membantu orang-orang mengelola keuangan mereka dan menciptakan sistem kesejahteraan yang lebih aman dan efisien, mencegah penipuan dan meningkatkan kepercayaan antara warganegara dan pemerintah. Pemerintah Inggris juga mempertimbangkan bagaimana teknologi blockchain bisa membantu warganegara untuk melacak alokasi dan pengeluaran dana dari pemerintah, donor atau organisasi bantuan kepada penerima yang sebenarnya, dalam bentuk hibah, pinjaman, dan beasiswa.

Potensi dan Dampak

Penerapan teknologi blockchain di dalam administrasi publik bisa mendorong proses-proses internal yang lebih efisien, mengurangi biaya transaksi, interaksi yang lebih dipercaya dan memudahkan pertukaran data antar organisasi dan berbagai lembaga pemerintah, serta mengurangi kemungkinan terjadinya berbagai kesalahan dan pemalsuan. Beberapa proses juga dapat diotomatisasi melalui *smart contract*. Namun, ada juga risiko yang harus diperhatikan. Pertama, untuk bisa menggunakan sistem baru berbasis digital, dibutuhkan biaya yang tidak murah, mulai untuk pemngembangan, pengelolaannya, perawatan hingga pelatihan untuk mengoperasikannya. Kapabilitas petugas sanagat krusial jika teknologi blockchain akan diterapkan sehingga pengelolaan buku besar sesuai dengan standar yang berlaku.

Meskipun buku besar blockchain dapat mencatat waktu dan rincian transaksi, mereka tidak dapat memverifikasi keakuratan apa yang dijelaskan di dalamnya. Selama transaksi sesuai dengan protokol persyaratan teknis, itu akan menjadi bagian yang tidak dapat diubah dari catatan, terlepas dari kebenaran isinya. Tidak berbeda dengan permintaan informasi dan yang diajukan ke lembaga-lembaga publik selama ini, tetap diperlukan prosedur seperti pemeriksaan dan lain sebagainya untuk memastikan kontrol yang cukup sebelum informasi didistribusikan kepada pemohon melalui blockchain.. Meskipun mungkin, suatu hari nanti teknologi blockchain bisa mengotomatisasi dan menjamin keamanan pelayanan tersebut tetap diperlukan aparat, karena blockchain tidak ditujukan untuk mengganti manusia melainkan melengkapai aparat untuk mengerjakan tugasnya dalam melayani publik menjadi lebih baik.

Fakta bahwa data dalam blockchain tidak dapat diubah - yang berarti bahwa data tidak dapat diubah atau dihapus setelah dimasukkan - memberikan transparansi dan akuntabilitas. Namun, ini juga dapat membahayakan privasi dan perlindungan data, terutama ketika menyangkut data pribadi atau sensitif (yang tidak boleh disimpan di blockchain). Blockchain tidak menjamin anonimitas dan, semakin pribadi datanya, semakin mudah untuk mengidentifikasi individu yang bersangkutan. Ketidakmampuan ini dapat mengancam 'hak untuk dilupakan/ *right to be forgotten*', di mana pengguna dapat, menuntut agar data pribadi mereka dihapus, dalam keadaan tertentu.

Sangat penting untuk memastikan bahwa semua warga negara dapat mengakses layanan publik . Meski begitu masih adanya kesenjangan digital menjadikan penerapan blockchain ini membawa resiko. Warga yang tidak dapat menggunakan layanan internet untuk alasan apa pun mungkin tidak dapat mengambil keuntungan langsung dari perkembangan blockchain yang akan memberi mereka kontrol lebih besar atas data dan transaksi mereka. Dan jika hal tersebut terjadi tentu saja nilai-nilai positif yang ditawarkan teknologi blockchain tersebut tidak akan bisa bermanfaat bagai seluruh masyarakat. Perlu dicatat bahwa inisiatif blockchain juga menjadi promosi yang tepat bagi pemerintah untuk mengubah pandangan terhadap lembaga pemerintah yang sentralistik dan tradisional khususnya dalam penyediaan layanan publik. Sementara layanan 'statelike' berbasis blockchain yang ditawarkan lembaga-lembaga non-pemerintah juga mulai berkembang yang pasti akan lebih menarik bagi masyarakat sehingga pada akhirnya akan menjadi tantangan yang tidak sederhana bagi suatu negara.

Kebijakan Antisipatif

Administrasi publik cenderung ingin mempertahankan kontrol pusat yang besar dan menginginkan bisa mengakses sistem blockchain secara *un-authorized* (*backdoors*) meskipun hal tersebut menghadirkan kerentanan keamanan baru. Pertanyaannya apakah pemerintah siap menerima dan mengakui hadirnya berbagao layanan 'statelike' yang independen di dalam otoritas mereka atau mau mempertimbangkan penerapan blockchain yang menawarkan kemampuan untuk meningkatkan berbagai layanan publik bagi warganya.



Kharim Indra Gupta Siregar

CIO PT. Bank Tabungan Pensiunan Nasional Tbk (BTPN)

Tentang Role CIO

> "Dulu pada masa awal menjadi CIO, pekerjaan tim IT adalah lebih banyak terkait penyediaan fungsi-fungsi baru, namun saat ini lebih banyak pada bagaimana memastikan layanan dengan kualitas dan performa yang baik setiap saat dimana saja dan kapan saja dan ini menuntut perubahan mindset."

iCIO Magz: Apa yang menjadi fokus Anda dalam satu tahun terakhir?

Kharim Siregar: Inisiatif IT yang merupakan bagian dari *key strategic initiative* BTPN untuk menciptakan perubahan khususnya dalam membangun landasan perbankan baru berbasis teknologi dengan tujuan memberikan layanan yang mudah dan terbaik kepada nasabah. Kalau melihat *project*-nya adalah digital banking yang sampai saat ini juga belum selesai karena ini bukan merupakan akhir tapi justru titik awal di mana semua bagian lain di BTPN juga harus berubah.

iCIO Magz: Apa yang menjadi keyakinan top level manajemen BTPN sehingga inisiatif IT menjadi bagian *key strategis inisiative*?

Kharim Siregar: Kalau kita lihat diawalnya apa yang dilakukan oleh teknologi itu adalah mengotomatisasi proses-proses *existing* yang selama ini dilakukan secara manual, jd tidak sekedar otomatisasi tetapi juga proses-proses baru yang di- *create* dengan menggunakan teknology. Dan seiring perkembangan teknologi khususnya *mobile*, saat ini hampir semua interaksi dengan pelanggan atau nasabah dapat dilakukan dengan teknologi untuk memberikan kemudahan-kemudahan yang baru, baik dari sisi nasabah maupun dari perbankan sendiri. Penerapan IT diperbankan meningkatkan efisiensi dalam memberikan layanan. Jadi teknologi sangat erat dengan proses. Kalau selama ini semua dilakukan oleh *people* dengan teknologi bisa dimasukkan di dalam logika program, dengan demikian fungsi dan tanggung jawab IT menjadi sangat besar ke depan.

iCIO Magz: Anda dipercaya menjadi CIO BTPN sejak 2008 ketika digitalisasi mulai populer. Apa perubahan role CIO yang Anda alami. Seperti apa perubahan tugas dan tanggung jawab IT yang ke depan Anda katakan akan semakin besar?

Kharim Siregar: Saya bersyukur di posisi ini sekian lama karena role teknologi berkembang bersama seiring sejalan dengan bisnis BTPN, dimana diawal hanya otomasi sekarang menjadi penentu utama layanan dengan menjadi digital. Dengan demikian role CIO juga berubah seiring tuntutan digital yang makin tinggi. Dulu pada masa awal menjadi CIO, pekerjaan tim IT adalah lebih banyak terkait penyediaan fungsi-fungsi baru, namun saat ini lebih banyak pada bagaimana memastikan layanan dengan kualitas dan performa yang baik setiap saat dimana saja dan kapan saja dan ini menuntut perubahan *mindset*. Hal ini sangat terasa ketika hampir semua layanan ada di aplikasi yang menjadikan hilangnya perantara antara *output* teknologi dan *user*. Sebelum era layanan perbankan berbasis aplikasi ini ketika sistem IT bermasalah, kami masih bisa mengatakan bahwa pelanggan tetap bisa mendapatkan pelayanan di kantor cabang secara manual. Sistem IT saat itu sudah menjadi sangat penting tetapi belum menjadi seratus persen *critica*l. Tetapi saat ini sistem IT adalah layanan perbankan itu sendiri karena melalui teknologi – aplikasi semua layanan itu disampaikan ke semua pelanggan. Dengan kata lain jika sistem IT tidak berfungsi maka layanan perbankan juga terhenti.

iCIO Magz: Menurut Anda akan seperti apa role seorang CIO lima tahun ke depan?

Kharim Siregar: Akan sangat tergantung masing-masing organisasi

dan perusahaannya. Seperti kita ketahui saat ini di era consumerization dari teknologi saat ini menuntut orang-orang bisnis yang tidak mengetahui IT menjadi harus memahami. Ekstremnya jika regulasi, security dan hal-hal lain memungkinkan semua pengembangan produk-produk digital banking akan dijalankan oleh bisnis dan layanan teknologinya akan dialihkan ke cloud provider.

Transformasi Digital

iCIO Magz: Bagaimana Anda dan manajemen meyakinkan anggota tim dan karyawan terkait inisiatif digital banking tersebut ?

Kharim Siregar: Meyakinkan dan mengajak tim di BTPN untuk berkontribusi karena inisiatif ini merupakan paduan unik dari penerapan teknologi mutakhir dan proses perbankan terkini. Meyakinkan bahwa inisiatif ini adalah suatu kesempatan langka dalam menciptakan suatu perubahan khususnya dalam membangun landasan perbankan baru berbasis teknologi untuk memberikan layanan yang mudah dan terbaik kepada nasabah. Pada awal 2009 ketika BTPN belum online sama sekali untuk bisnis yang dijalankan yakni untuk pensiunan. Ketika itu kami baru memperkenalkan bisnis baru yakni mikro. Saat itu ada sekitar 450 cabang yang harus di *online*-kan dari sekitar 600 cabang mikro yang harus dikembangkan dalam waktu 9 bulan. Ppara pensiunan yang menjadi nasabah memiliki perilaku dimana setiap awal bulan datang berbondong-bondong ke bank untuk mengambil uang pensiun. Waktu itu sistem mati. Paginya membaca berita di koran seorang perempuan yang telah lanjut usianya tertidur dengan dikelilingi enam orang cucunya di bagian belakang angkot. *Headline* berita itu adalah: Penderitaan seorang nenek dancucunya yang gagal mengambil uang pensiun karena sistem BTPN mati. Saat itu sebagai profesional saya merasa gagal dan mengambil pelajaran penting bahwa selaku profesional kita harus memposisikan sebagai diri sebagai pelanggan. Koran itu masih saya kliping dan simpan sampai saat ini dan selalu saya tunjukkan kepada anggota tim yang baru bergabung agar mereka memahami kalau sistem IT di BTPN terkena gangguan dan mati, efeknya sangat besar dan langsung berdampak kepada para pensiunan yang sebagian besar tidak memiliki alternatif lain seperti kartu kredit.

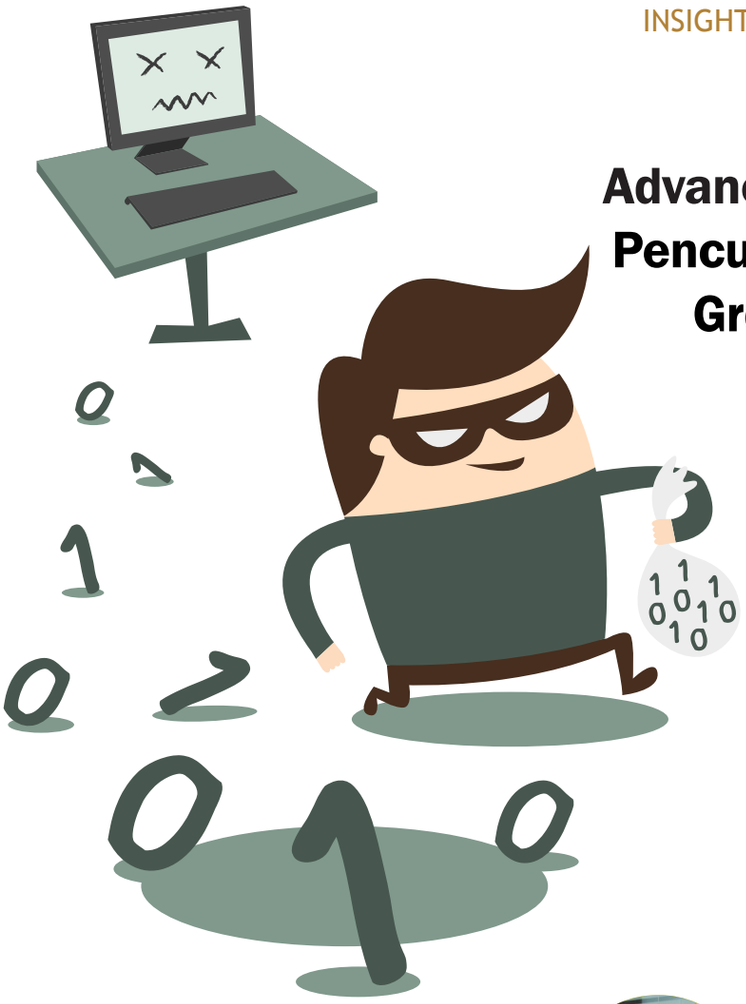
iCIO Magz: Apa tantangan utama BTPN bertransformasi menuju digital banking?

Kharim Siregar: Bagi saya transformasi digital adalah Menjawab masalah yang dihadapi pelanggan dengan meng-*utilize* teknologi. Tantangan paling utama menuju digital banking adalah mengubah pola pikir (*mindset*). Perubahan *mindset* dilakukan, baik dari internal divisi IT, internal bank, maupun mitra pendukung yang harus bekerja sama dengan bank untuk memberikan produk dan layanannya. Untuk itu BTPN berusaha meyakinkan dan mengajak tim di BTPN untuk berkontribusi sepenuhnya karena inisiatif ini merupakan paduan unik dari penerapan teknologi mutakhir dan proses perbankan terkini.

iCIO Magz: Seperti apa sebenarnya digital banking yang ingin dituju BTPN?

Kharim Siregar: Pada dasarnya adalah pelanggan dapat menjalankan semua layanan perbankan yang dibutuhkannya pada saat pelanggan tersebut membutuhkan. Contoh produk bank saat ini bagi saya, anda dan pelanggan adalah sama, dengan adanya digital tidak hanya teknologinya saja tapi juga digabungkan dengan kemampuan analitik dan sebagainya sehingga memampukan pelayanan kepada setiap orang berdasarkan pada interaksinya dengan bank. Misalkan nasabah yang memiliki tabungan dengan nilai yang banyak, diberikan bunga tabungan yang lebih tinggi. Atau nasabah yang lebih sering memanfaatkan layanan untuk bertransaksi akan mendapatkan fasilitas yang berbeda dengan yang jarang memanfaatkannya. Intinya adalah cara kita melihat produk perbankan seperti saat ini akan hilang . Layanan digital banking adalah tailor made yang berbeda-beda setiap nasabah berdasarkan profil mereka dan itu bisa dilakukan secara *realtime*.

Dan untuk mewujudkan hal tersebut membutuhkan komitmen dari semua yang terlibat, mulai top level manajemen hingga paling bawah. Setelah itu langkah berikutnya adalah jangan melihat apa yang dilakukan saat ini, tapi dengan teknologi baru yang ada bagimana kita bisa merancang layanan-layanan baru. Karena kalau kita mau mengubah layanan yang sudah ada dengan teknologi baru pasti akan lebih banyak kompromi nya. Untuk mewujudkan digital banking tidak semata perlu uang/modal tetapi juga *skill* dan kapabilitas tim secara menyeluruh mulai *programmer*, *security*, *operation*, *services* dan lainnya. Namun idealnya perubahan tersebut dilakukan secara bertahap dan dimulai di unit atau divisi tertentu terlebih dahulu secara total. Setelah itu dijadikan lesson learned untuk melakukan perubahan di unit/ divisi bisnis lainnya.



Advanced Persistence Threat: Pencuri dengan Kemampuan Group Ocean's Eleven

*Apakah anda pernah menonton film Ocean's Eleven (2001) yang dibintangi oleh George Clooney, Matt Damon, Brad Pitt dan Julia Roberts? Film dengan latar belakang pencurian kasino tersebut sampai dibuat 2 seri beruntun setelahnya, yaitu Ocean's Twelve (2004) dan Ocean's Thirteen (2007) dan Ocean's 8 yang saat tulisan ini dibuat sedang diputar di bioskop di berbagai kota. Film yang berkisah tentang pencurian yang dilakukan oleh orang-orang professional dan terlatih, dimana targetnya amat spesifik dengan memakan waktu persiapan dan pelaksanaan amat panjang. Seperti itulah kira-kira Advance Persistence Threat (APT), dimana bentuk serangan (*Threat*) terbilang sangat canggih (*Advanced*) karena dilakukan oleh orang-orang atau kelompok yang memiliki kemampuan sangat baik, serta ditujukan kepada target yang spesifik dan terus-menerus (*Persistence*). Apakah kita siap dan memiliki kemampuan untuk menangkal serangan seperti ini? Atau, seberapa berharga aset yang kita miliki, sehingga kita menjadi target dari serangan berbasis APT?*



Toto A. Atmojo
CEO PT Defenxor Nusa Semesta

Pertengahan Februari 2018 lalu, dunia dikejutkan oleh keterangan dari Robert Mueller, mantan direktur FBI yg ditunjuk sebagai ketua dari konsil yang dibentuk untuk menyelidiki keterlibatan Rusia, yang menyimpulkan bahwa 13 individu Rusia terlibat dalam menginterferensi pemilu Amerika Serikat tahun 2016. Hal ini menambah panjang daftar bukti dan kasus keterlibatan Rusia dalam pemilu tersebut, dengan tujuan memenangkan Trump. Pada beberapa kejadian yang diungkap, terlihat bahwa serangan ditujukan kepada tim kampanye Hillary Clinton dan anggota dari Partai Demokrat. Serangan tersebut sangat spesifik ditujukan kepada target yang khusus, dengan metode yang amat canggih yang bahkan belum ditemukan sebelumnya, sehingga disebut sebagai *Advanced Persistence Threat* (APT).

Serangan berbasis APT terhadap pemilu presiden di Amerika Serikat di atas, memiliki karakteristik yang sama dengan serangan berbasis APT yang lain. Sebagai contoh serangan Stuxnet yang menyasar fasilitas pengayaan uranium Iran, dengan Amerika Serikat dan Israel dipercaya sebagai dalang dibelakangnya dengan kode operasi: *Operation Olympic Games*. Meski malware ini terdeteksi 'beredar' di beberapa negara (termasuk Indonesia diurutan kedua sebesar 18.2%), stuxnet disebutkan mentargetkan fasilitas nuklir Iran. Stuxnet tidak menyebabkan kerusakan pada sistem yang bukan menjadi targetnya, karena secara spesifik mentargetkan *Programmable Logic Controllers* (PLCs) yang dipakai dalam sentrifugal untuk memproduksi material nuklir Iran dan berada di sana tanpa terdeteksi selama bertahun-tahun. Serangan ini disebutkan mampu menghambat program nuklir Iran selama 4 tahun, lebih efektif dari serangan bom yang hanya menghambat program tersebut selama 3 tahun saja. Film berjudul Zero Days yang dirilis tahun 2016 menceritakan Stuxnet dengan cukup detail.

Ada lagi Operation Aurora yang menyasar puluhan perusahaan besar IT, seperti Google, Adobe, Juniper serta perusahaan lain pada sektor teknologi, finansial dan *defense*. Serangan ini dipercaya dilakukan oleh Cina, dengan tujuan untuk mencuri *intelectual property* berupa *source code* dari perusahaan yang menjadi target, juga untuk membungkam aktivis pro demokrasi di Cina. Serangan ini mengeksploitasi kelemahan pada software Internet Explorer dan Adobe Acrobat Reader yang sebelumnya belum pernah ditemukan (0-Day *vulnerability*). Serangan ini juga menggunakan beberapa level enkripsi serta beberapa jenis malware untuk mengelabuhi dan mencegah terdeteksi. Operation Aurora dipercaya berlangsung sejak pertengahan 2009 dan baru dideteksi awal tahun 2010 oleh Google.

Di masa mendatang, kita akan melihat semakin banyak serangan berbasis APT, terutama yang disponsori dan di *backup* oleh negara. Hal tersebut karena serangan jenis ini dilihat lebih murah biayanya dibandingkan dengan serangan secara fisik seperti peperangan. Pun soal risikonya terhadap penyerang yang juga minim, karena pelakunya sulit dibuktikan secara nyata.

Advanced & Persistance

Serangan APT merupakan serangan yang *Advanced*. Baik dari sisi jenis serangan, maupun tekniknya. Sebagai contoh adalah Stuxnet, dimana worm ini menyasar sistem *Supervisory Control and Data Acquisition* (SCADA) berbasis PLC, yang dikenal sebagai sistem yang tidak dikenal secara luas. Sistem ini berbeda dengan target berbasis OS yang umum ada di pasaran, seperti Windows maupun Linux. Hal ini terjadi karena serangan APT menyasar target yang spesifik, bukan seperti serangan jenis malware pada umumnya yang mentargetkan sebanyak-banyaknya korban, sehingga dibuat berdasarkan sistem yang paling banyak dipakai.

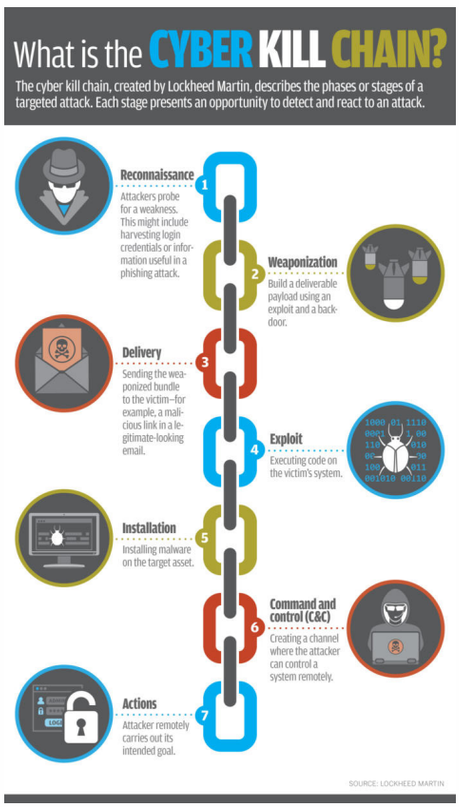
Salah satu contoh jenis serangan yang sering dipergunakan dalam APT adalah Zero Day atau 0-Day. Awalnya istilah 0-Day adalah untuk jenis kelemahan pada sistem (*bug* atau *vulnerability*), yang dapat dieksploitasi dan belum dikeluarkan *patch* oleh pembuat sistem tersebut. Kelemahan berbasis 0-Day bahkan hanya diketahui oleh si pembuat *exploit*. Dengan memiliki *exploit* berbasis 0-Day, dapat dipastikan serangan akan berhasil terhadap target yang ditentukan. Namun saat ini juga terdapat 0-Day Virus, dimana sebuah virus yang belum bisa di deteksi oleh Anti Virus yang ada.

APT juga memiliki sifat yang *persistance*, dimana dilakukan dalam kurun waktu yang lama dan hanya menyasar institusi atau individu tertentu. Penyerang melakukan studi secara spesifik mengenai target serangan, untuk melihat profil dan kelemahan yang ada. APT tidak mentargetkan sebanyak-banyaknya korban seperti virus atau ransomware pada umumnya, karena memang tujuannya spesifik serta mencegah selama mungkin untuk terdeteksi.

Sebagai contoh serangan dengan jenis virus yang memang secara khusus ditujukan untuk institusi tertentu, dan tidak berjalan pada lingkungan lainnya. Misal hacker sudah mengetahui bahwa setiap nama komputer di perusahaan kita, memiliki format XYZ-[NAMA-DIVISI]-[NOMOR-WORKSTATION]. Maka dibuatlah virus baru yang hanya berjalan di komputer dengan format nama target di atas (nama komputer memiliki awalan XYZ-), dan tidak berjalan di target lainnya. Hal ini tentu amat menyulitkan bagi proteksi yang basisnya tradisional, seperti berbasis *Signature*.

Pendekatan untuk serangan APT

Dalam menangani APT, dapat dilakukan beberapa pendekatan yang ada. Salah satunya adalah pendekatan yang di usulkan oleh Lockheed Martin (LM) dalam papernya yang berjudul "*Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*". LM mencoba untuk membagi serangan menjadi beberapa tahapan, untuk kemudian di terapkan langkah-langkah yang tepat pada tahapan tersebut. Pendekatan ini sebenarnya tidak spesifik untuk serangan berbasis APT, namun juga untuk serangan yg sifatnya tradisional lainnya. Tahapan yang dimaksud adalah Cyber-Killchain:



Gambar 1. Tahapan pada Cyber Kill Chain
(Sumber: www.csoonline.com)

Pada gambar di atas, terlihat bahwa tujuan akhir dari penyerang adalah *Action*. Hal ini bisa berupa banyak hal, mulai dari pencurian data, membuat sistem tidak berfungsi (*Denial of Service*), atau bahkan merusak sistem secara keseluruhan. Semakin kita dapat mendeteksi dan menangkal serangan pada fase awal, maka semakin baik. Tujuan utama dari pendekatan yang kita lakukan adalah sedapat mungkin mencegah serangan pada fase Action. Sebagai contoh ekstrim adalah, jika komputer sudah terlanjur terinfeksi virus (*Fase Installation*), maka sedapat mungkin dicegah terkoneksi ke C&C, sehingga tujuan virus tersebut dibuat (Action on Target) tidak tercapai.

Pada masing-masing tahapan serangan di atas, LM juga menganjurkan beberapa tindakan atau perangkat yang diperlukan, berdasarkan tindakan yang ingin kita lakukan pada setiap tahapan tadi (jika dimungkinkan). Tindakan yang dimaksud adalah: *Detect, Deny, Disrupt, Degrade, Deceive, Destroy*. Misal jika kita ingin mendeteksi serangan pada fase Exploitation, maka diperlukan *Host Intrusion Detection System* (HIDS). Detail matrix tindakan pada setiap tahapan serangan ada pada gambar dibawah ini:

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Gambar 2. Matriks tindakan pada setiap tahapan serangan (Sumber: Lockheed Martin)

Tindakan yang diusulkan LM di atas tentu saja dapat dikembangkan, sesuai dengan sifat APT dan kondisi yang ada di lingkungan kita. Sebagai contoh, untuk mendisrupsi Virus yang merupakan 0-Day pada tahapan *installation*, bisa menggunakan teknologi *sandboxing*. Dengan *sandboxing* kita dapat mengeksekusi atau membuka *file* yang dicurigai mengandung virus namun tidak terdeteksi oleh *signature AV*, pada lingkungan yang aman namun serupa dengan lingkungan sesungguhnya. Jika ternyata *file* tersebut merusak, maka 'lingkungan' tadi (biasanya simulator dari OS) bisa kita *delete* dengan mudah.

Meskipun telah memberikan landasan yang baik untuk memetakan tahapan serangan, serta tindakan pada setiap tahapan tersebut, LM tidak memberikan petunjuk tentang siapa yang perlu melakukan tindakan pada tiap serangan. Seperti kita ketahui, *security* haruslah komprehensif, dimana mencakup: **Technology, People & Process**. Jika dilihat, proses pencarian dan pendeteksian serangan pada berbagai fase Cyber Killchain memerlukan keahlian yang khusus. Teknologi dapat memudahkan kita pada level tertentu, misalnya dengan adanya Artificial Intelligence maupun *automation*, namun tetap harus ada peranan manusia dalam setiap tindakan. Diperlukan personil yang memiliki kemampuan dalam mendeteksi serangan, serta menyimpulkan apakah serangan ini valid atau tidak. Terlebih lagi jika yang dihadapi adalah APT, hal ini tentu menjadi lebih sulit dan kebutuhan akan personil yang mumpuni tentunya lebih besar lagi.

LM tidak menginformasikan, siapa yang perlu melakukan analisis jika terdeteksi adanya serangan yang 'tidak biasa'. Padahal untuk mendeteksi dan mengolah serangan berbasis APT, diperlukan personil *IT Security* yang memiliki kemampuan sangat baik. Sebagai contoh Stuxnet, dimana dideteksi dan diteliti oleh berbagai ahli IT Security dari Symantec dan Kaspersky Lab yang memiliki sumber daya (*Tools*, *lab*, jaringan ahli & pengetahuan) serta personil yang setiap hari bergelut dengan serangan dan virus. Pertanyaannya, apakah kita memiliki sumber daya seperti Symantec & Kaspersky Lab? Hal ini tentu perlu disiasati lebih lanjut, karena mencari personil *IT Security* yang baik tentu tidak mudah dan pastinya tidak murah. Terlebih lagi jika kita ingin memastikan keamanan selama 24/7, yang membutuhkan personil *standby* 24/7 pula.

Serangan pada umumnya

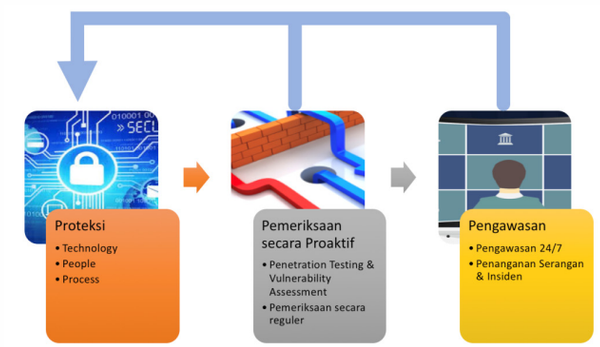
Apakah kita perlu menyiapkan pertahanan untuk menanggulangi serangan berbasis APT? Jawabannya bisa ya dan tidak. Namun pertanyaan sebelumnya adalah: Apakah anda yakin memiliki aset yang diincar oleh penyerang berbasis APT? Karena tidak mungkin tim Ocean's Eleven akan merampok bandar Judi Togel (Toto Gelap), karena kelasnya mereka adalah merampok kasino besar di Las Vegas.

Berdasarkan pengamatan kami di Security Operation Center Defenxor, yang memonitor keamanan puluhan institusi dan perusahaan selama 24/7, kebanyakan serangan bukanlah serangan yang spesifik (*Persitance*) meskipun ada beberapa yang cukup *Advanced*. Serangan yang ada sebenarnya dapat terdekteksi dan dicegah, namun perlu *tunning* dan penanganan lebih lanjut. Sebagai contoh perusahaan telah mengimplementasikan *Web Application Firewall* (WAF), namun masih terjadi insiden *defacement* dimana halaman web diganti. Setelah diselidiki, ternyata ada policy pada WAF yang perlu di *tunning*. Ada pula perusahaan yang *Intsusion Prevention System* (IPS), namun *policy*nya masih *allow-all* yang berarti tidak mem-*Prevent* apapun. Bahkan masih sering

kami dapati *traffic ransomware wannacry* yang cukup menghebohkan di pertengahan 2017.

Kesimpulan dan Saran

Lalu apa yang harus kita lakukan untuk mengetahui apakah kita sudah terkena serangan berbasis APT? Jika pertanyaan ini ditanyakan ke saya, maka jawabannya adalah: Berdoa yang banyak..:) Jika memang kita menjadi target serangan dengan profil penyerang sedemikian canggih dan *targetted*, apakah kita punya sumber-daya untuk mendeteksi dan menangkal serangan semacam itu? Namun pertanyaan berikutnya, apakah kita memiliki aset yang sedemikian berharga sehingga menjadi target serangan APT? Sekali lagi, saya yakin group perampok Ocean's Eleven tidak akan merampok target yang tidak memiliki aset berharga menurut ukuran mereka.



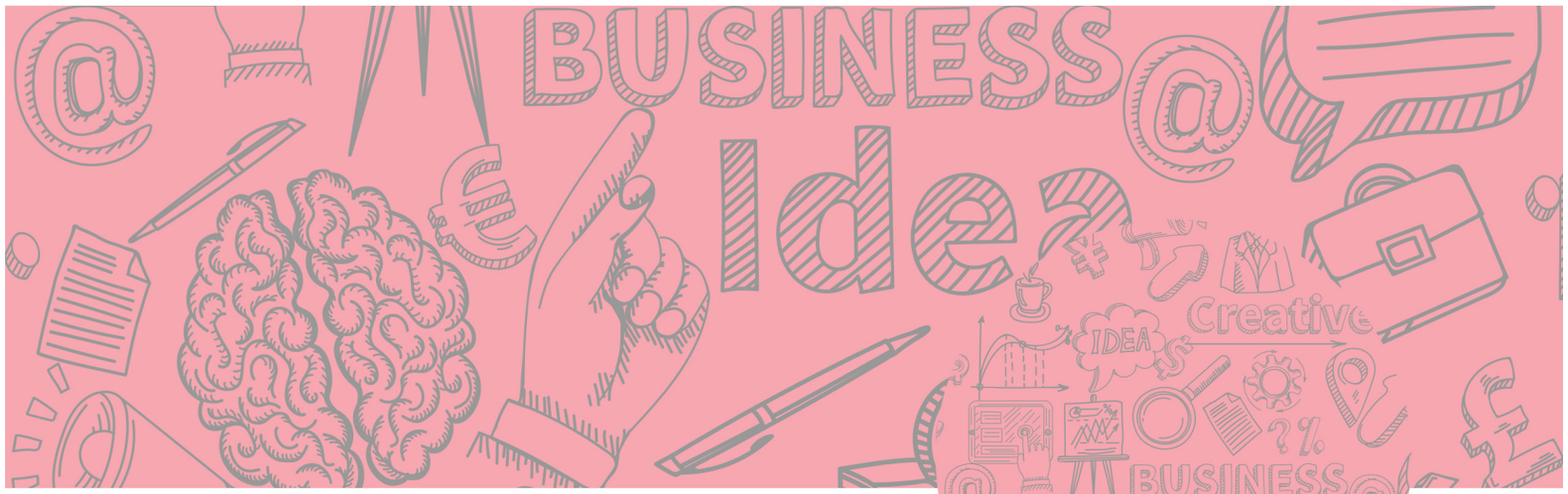
Gambar 3. Pendekatan Keamanan Informasi

Oleh karena itu kita perlu terlebih dahulu melakukan *assessment* terhadap aset yang kita miliki, berapa nilainya, apa saja risiko terkait aset tersebut dan berapa kerugiannya jika risiko menjadi kenyataan (*tangible* maupun *intangible*). Setelah dilakukan *assessment*, maka selanjutnya kita terapkan proteksi untuk menjaga agar risiko tidak menjadi kenyataan. Framework Cyber Killchain dari LM diatas dapat menjadi acuan untuk melakukan **Proteksi**, berdasarkan tahapan serangan dan tindakan pada setiap tahapan tersebut. Proteksi disini tidak terbatas hanya pada implementasi **Teknologi** saja, namun juga terkait **People** (*user awareness*, kemampuan personil IT Security, dll) dan juga **Process** (*Policy, Procedure & Guideline*). Dengan melihat risiko dan mencocokkan proteksi yang ada terkait risiko tersebut, maka kita terhindar dari implementasi teknologi yang tidak tepat, baik yang kurang maupun berlebih.

Setelah kita menerapkan proteksi yang kita anggap sesuai, maka berikutnya adalah melakukan pemeriksaan apakah proteksi sudah sesuai untuk mencegah terjadinya risiko. Pemeriksaan ini bisa berupa *vulnerability assesment* atau *penetration testing*, dimana kita mensimulasikan serangan yang dilakukan oleh hacker sesungguhnya. Jika berdasarkan hasil pemeriksaan ada yang perlu diperbaiki, kita dapat kembali lagi ke tahapan proteksi sebelumnya.

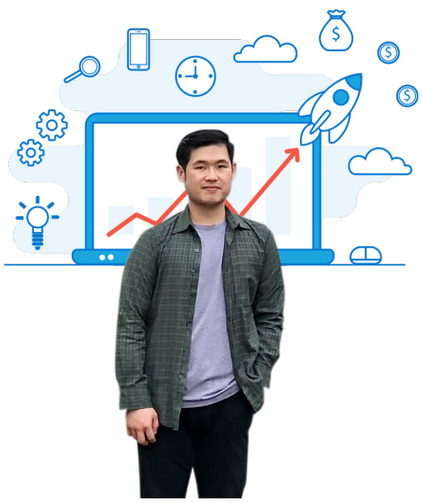
Pada akhirnya, perlu dilakukan *monitoring* keamanan selama bisnis berjalan. Hal ini bertujuan untuk mendeteksi jika terjadi serangan yang masih lolos, juga untuk tujuan penanganan jika insiden sudah terjadi (Forensik). *Monitoring* dan deteksi ini dapat dilakukan dengan mengimplementasi *Security Operation Center* (SOC), atau bekerjasama dengan pihak ketiga yang menyediakan layanan SOC tanpa kita perlu implementasi sendiri. Implementasi SOC (baik secara mandiri maupun lewat pihak ketiga) menjadi pilihan yang tepat, karena fungsinya yanng melakukan monitoring selama 24/7 dengan gabungan antara Technology, People & Process. Kapabilitas SOC yang baik juga secara empiris terbukti secara signifikan memiliki positif terhadap kinerja keamanan informasi.

APT merupakan serangan yang sangat kompleks dan canggih, dimana mungkin kita tidak memiliki sumber daya untuk menanggulanginya. Jika kita memang menjadi target dari serangan APT dimana kita memiliki aset yang menjadi sasarannya, seharusnya kita memiliki sumber daya untuk mendeteksi dan menanggulangi serangan tersebut. Karena logikanya, tidak mungkin pengamanan kasino ternama di Las Vegas sama dengan pengamanan bandar judi toto gelap. Sementara itu, setidaknya kita harus terproteksi dari jenis serangan yang memang menyasar semua institusi seperti *ransomware*, *defacement*, virus, dll. Memang, tidak ada celah keamanan yang terlalu kecil untuk diacuhkan dan dibiarkan terbuka. Namun pendekatan implementasi keamanan berbasis risiko, serta perencanaan yang matang amat penting, untuk mencegah harga brankas lebih mahal dari isinya.



Siapkan BCP dan DR Antisipasi Potensi Gangguan Bisnis di Tahun Politik

Selain technology, business continuity plan dan disaster recovery membutuhkan people dan process. Dua hal yang sering terabaikan ini menjadi penentu optimal atau tidaknya investasi solusi teknologi ini untuk mengantisipasi berbagai ancaman baik yang disebabkan oleh faktor alam maupun manusia.



Andika Halim
Team Leader Database PT. Inovasi Informatika Indonesia

Seperti yang menimpa Komisi Pemilihan Umum (KPU) dan Badan Pengawas Pemilu (Bawaslu) di pilkada serentak 2018 baru-baru ini. Kedua situs lembaga yang bertanggung jawab dalam penyelenggaraan dan pengawasan pemilu itu sempat diretas oleh para *hacker*. Meskipun tidak sampai berdampak pada hasil akhir pemilu, kejadian ini tentu menjadi peringatan bagi pemerintah untuk lebih mempersiapkan keamanan berbagai fasilitas *online*, khususnya situs KPU maupun Badan Pengawas Pemilu (Bawaslu) secara matang. Terlebih hajatan lima tahunan yakni pilpres 2019 akan segera dimulai.

Di sisi lain lancarnya penyelenggaraan pilkada serentak tanpa disertai gejolak politik apalagi kerusuhan tentu menjadi pertanda yang baik bagi perekonomian yang harus diantisipasi oleh para pelaku usaha dalam upaya untuk memberikan pelayanan terbaik bagi para pelanggannya. Jangan sampai situs atau *website* perusahaan mengalami insiden yang sama dengan yang dialami salah satu situs *e-commerce* terbesar di Indonesia pada bulan Mei lalu. Saat itu banyak sekali pelanggan yang ingin bertransaksi mengalami gagal koneksi karena ketidaksiapan toko online tersebut mengantisipasi peningkatan traffic sebagai respon pelanggan terhadap berbagai program belanja yang disediakan seperti *flash sale* dan berbagai promo lainnya.

Cerita itu disampaikan kembali oleh Andika Hakim, team leader database PT. Inovasi Informatika Indonesia untuk menggambarkan pentingnya *business continuity plan* (BCP) dan *disaster recovery* (DR) di dalam sistem IT. Apalagi menurut Andika potensi gangguan yang mungkin dialami oleh perusahaan dan menyebabkan bisnis tidak bisa beroperasi secara normal sangat banyak mulai bencana alam seperti banjir, gempa bumi, dan kebakaran,

kecelakaan, sabotase, kehilangan energi, kegagalan dalam transportasi, komunikasi, keselamatan, dan sektor jasa lainnya, bencana lingkungan seperti polusi dan tumpukan material berbahaya, dan serangan *cyber* hingga aktivitas hacker.

Tantangan inilah yang dapat dijawab dengan mempersiapkan BCP dan DR secara lebih baik mulai dari perencanaan, implementasi, hingga pengelolaannya setelah dipergunakan.

Mengatasi Keterbatasan

Pentingnya BCP & DR untuk menjaga agar perusahaan tetap bisa menjalankan bisnis ketika terjadi insiden sebenarnya sudah sangat disadari, terutama oleh perusahaan yang membutuhkan *zero downtime*. Meski demikian masih banyak perusahaan yang memprioritaskan pengimplementasian solusi ini ke dalam sistem TI mereka.

Andika mengakui banyaknya persyaratan yang harus dipenuhi perusahaan menjadi sumber keengganan perusahaan menerapkan solusi BCP/DR. "Padahal di era digital ini perusahaan dituntut untuk terus memiliki daya saing agar bisa bertahan dan terus tumbuh."

Hasil survei Evolveip pada tahun 2017 terhadap responden di industri *banking*, teknologi, kesehatan, manufaktur, dan pendidikan, mereka menyatakan siap menyelamatkan aset TI mereka apabila ada terjadi insiden. Namun, dengan banyaknya persyaratan yang harus dipenuhi oleh perusahaan untuk menerapkan solusi ini, hanya kurang dari setengah industri tersebut yang merasa siap menjadikan *disaster recovery* bagian dari sistem TI mereka. Sementara penelitian Continuity Central, menyimpulkan 34,4% responden menganggap kurangnya anggaran dan sumber daya sebagai tantangan utama mereka untuk mengimplementasi BCP/DR akan menjadi tantangan utama mereka pada 2018. Tidak mengejutkan jika belanja solusi ini stagnan alias sama dengan tahun lalu.

Bagi banyak perusahaan, soal *people* dan *process* ini memang menimbulkan dilema tersendiri. Dari sisi *people*, tidak mudah menemukan orang yang memiliki kemampuan terhadap BCP/DR yang memadai. Apalagi teknologi juga berkembang sangat cepat yang menuntut para praktisi di bidang solusi ini terus beradaptasi. Sementara dari sisi proses dibutuhkan kerja ekstra keras untuk mengelola BCP/DR. Dukungan dari top level manajemen juga menjadi tantangan yang tak kalah serius. Apalagi, investasi di sisi teknologi dan sistemnya seringkali tidak murah. "Setiap tim sepakbola profesional menginginkan Messi, tetapi tidak ingin mengeluar biaya transfer yang sangat besar untuk menebusnya," kata Andika menganalogikan.

Di sini layanan *managed services* BCP/DR menjadi bisa menjadi alternatif. Dari sisi teknologi perusahaan dapat terus mengikuti perkembangan teknologi di ranag BCP/DR ini. Pun unsur *people* dan *process* ditangani oleh pihak ketiga selaku penyedia layanan.

Dari sisi *people* mereka punya tim ahli yang siap bekerja 24/7 untuk memastikan availability data. Sementara dari sisi proses, mereka juga memiliki SOP khusus ketika terjadi insiden baik karena faktor internal maupun eksternal.



Bisa Disiasati

Jika mengalihkan penerapan BCP/DR kepada pihak ketiga tidak menjadi pilihan, sejumlah cara bisa diterapkan untuk memangkas biaya yang dibutuhkan dalam mengimplementasikan solusi ini. Pertama mengeliminasi berbagai *idle asset* yang menjadi salah satu kontributor biaya terbesar dari *disaster recovery*. Maka, aset yang belum atau tidak digunakan, lebih baik disingkirkan atau dialokasikan di tempat yang berbeda, agar apabila terjadi bencana, aset-aset tersebut tidak terkena dampak dan membiarkan perusahaan mengeluarkan dana lebih untuk perbaikan aset tersebut.

Kedua standarisasi, ini mengingat seiring dengan perkembangan bisnis biasanya semakin banyak jenis teknologi yang digunakan, semakin banyak jumlah jenis sumber daya yang diperlukan untuk *disaster recovery*. Membatasi varian platform dan komponen infrastruktur, juga menentukan standar konfigurasi mengurangi kerumitan proses *disaster recovery* dan biaya yang tidak perlu.

Ketiga otomatisasi, dengan tujuan untuk menyederhanakan proses pengujian, meningkatkan keandalan, dan mendorong efisiensi dengan mengurangi waktu yang diperlukan untuk menyelesaikan tugas.

Keempat virtualisasi, yang merupakan cara yang paling berpotensi untuk menurunkan biaya BPC dan *disaster*

recovery. Virtualisasi dapat mengurangi penggunaan *devices*, mengurangi peralatan di *data center*, dan mengurangi kebutuhan daya.

Kelima, integrasi dengan sistem IT perusahaan secara keseluruhan. Jika tidak terintegrasi perusahaan akan mengeluarkan biaya lebih, khususnya untuk pihak ketiga untuk mengelola dan memelihara BPC dan *disaster recovery*. Mengintegrasikan fungsi BCP dan *disaster recovery* sebagai bagian dari perencanaan operasional sistem TI, dapat mengurangi biaya tersebut.

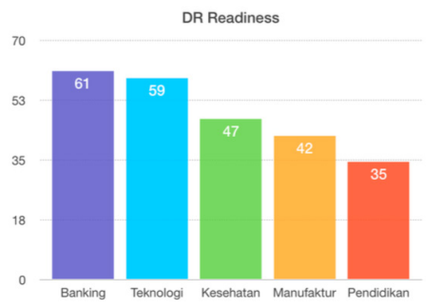


Keenam memperbaiki pendokumentasian. Buruknya pendokumentasian dalam sebuah perusahan akan memicu pembengkakan biaya saat perusahaan akan melakukan *disaster recovery testing*.

Ketujuh *testing* semua aset mulai jaringan, *server, storage*, dan komponen aplikasi tertentu untuk dapat membantu memastikan pemulihan telah tepat dan menghindari biaya tidak terduga jika pengujian salah satu aset gagal.

Aspek Lain yang Menentukan

Jika perusahaan telah siap untuk menerapkan BCP dan *disaster recovery*, CIO juga harus memperhatikan empat aspek penting yang sangat menentukan kesuksesan BCP dan *disaster recovery plan*, yaitu: *people*-mempersiapkan orang-orang dalam perusahaan yang terlibat langsung apabila bencana terjadi, *Property* - untuk menentukan perangkat-perangkat yang harus diselamatkan dan dijamin ketersediaannya apabila bencana terjadi, serta *Priorities - high availability* atau *zero downtime*.



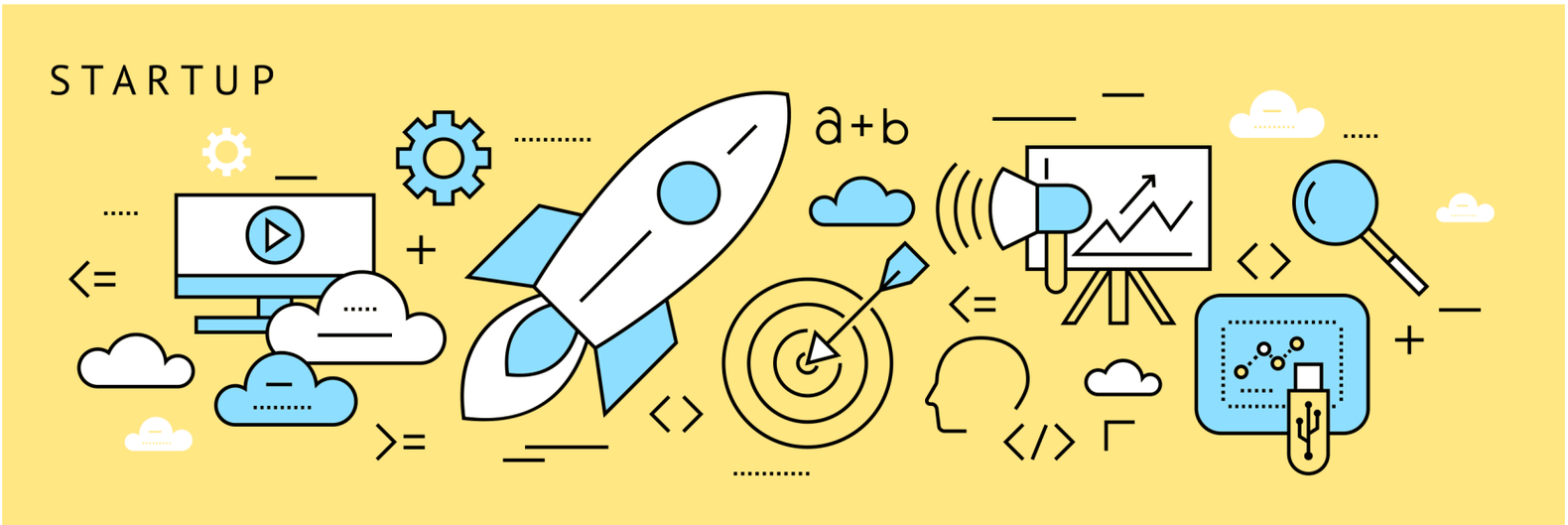
source: https://www.evolveip.net/

Namun, Andika mengungkapkan ada satu satu aspek tambahan yang tak kalah pentingnya, yaitu latihan (*practice).* "Investasi perusahaan terhadap solusi BCP dan *disaster recovery* akan percuma jika SDM tidak mendapatkan persiapan yang cukup untuk menerapkan solusi tersebut dengan tepat sesuai dengan prosedur dan kebijakan yang telah ditentukan," kata Andika.

Bank of Japan adalah contoh ideal terkait hal ini ungkap Andika. Sebagai bank sentral, Bank of Japan, menerapkan solusi BCP sebagai upaya untuk menghindari aktivitas perbankan dari gangguan. Sebagai bank sentral bagi negara yang rawan akan gempa, *Bank of Japan* terus mengembangkan dan memperbarui sistem BCP dan *disaster recovery* yang mereka miliki agar tugas dan tanggung jawab krusial seperti *payment system* dan *settlement system* tetap dapat dilakukan. Agar solusi ini berhasil, *Bank of Japan* juga memberi pelatihan kepada para stafnya dan melakukan latihan darurat secara berkala untuk memastikan bahwa para stafnya dapat memberikan tanggapan terhadap bencana secara tepat.

Dari usaha Bank of Japan, semakin menegaskan bahwa memberikan pelatihan yang tepat dan secara berkala untuk meningkatkan kemampuan SDM, juga dapat memberikan keuntungan bagi perusahaan. SDM dapat membantu meningkatkan perlindungan terhadap sistem TI perusahaan dan melindungi operasi bisnis dari kegagalan sistem apabila *downtime* atau gangguan akibat bencana terjadi. Hal tersebut juga akan mengurangi risiko hilangnya data. Memiliki SDM yang berkualitas juga akan membantu perusahaan untuk mengeliminasi ketergantungan perusahaan dari proses *disaster recovery* yang bersifat tradisional seperti *backup* dalam bentuk *tape* menjadi aktivitas backup yang lebih *up-to-date*. Biaya pengeluaran juga dapat dikurangi karena ketergantungan perusahaan terhadap pihak ketiga atau *vendor* TI ketika *downtime* terjadi juga dapat diminimalisir.

Semakin berkembangnya teknologi dan informasi di dunia, semakin membuat perusahaan harus terus berupaya agar mereka dapat bersaing dan menjalankan bisnis dalam keadaan apa pun. Terfokus hanya pada penerapan teknologi seperti BCP dan *disaster recovery* pada sistem TI tidak cukup untuk memastikan bahwa bisnis terhindar dari berbagai jenis gangguan ataupun *"disaster"*. Perusahaan juga harus mempertimbangkan apakah mereka telah memiliki SDM yang mampu memberikan respons secara tepat sesuai prosedur dan kebijakan yang ada.



Startup Makin Seksi Bisnis Venture Capital Tak Henti Berinovasi

Peran penting Venture Capital atau biasa disingkat VC bagi startup kadang terlupakan karena bisnis mereka memang 'dibelakang' layar. Namun bukan berarti bisnis ini sepi dari inovasi, mereka terus berbenah untuk bisa teus berkompetisi seiring perkembangan industri startup yang makin seksi

Industri startup tumbuh pesat. Dimulai dengan berkembangnya *e-commerce* sekitar lima tahun lalu, kini ribuan perusahaan rintisan tumbuh bak cendawan di musim penghujan untuk men-disrupsi bisnis konvensional. Data dari Startupranking.com menunjukkan, saat tulisan ini dibuat Indonesia menempati peringkat keenam di dunia dilihat dari jumlah startupnya di bawah Amerika Serikat, India, Inggris, Kanada, dan Jerman dengan jumlah perusahaan rintisan mencapai 1842. Nilai investasi di sektor ini juga terus meningkat. Laporan Google dan AT. Kerney menyebut jika pada 2016 nilai investasi di startup mencapai US 1.4 milyar dolar, pada periode Januari hingga Agustus 2017 tumbuh enam puluh delapan kali lipat menjadi US 3 milyar dolar.



Kelvin Yim
Executive Director & Founding Mentor AMI

Ya, seiring dengan menjamurnya perusahaan startup, industri VC- pengelola dana investasi yang menyasar perusahaan rintisan juga berkembang pesat. Nyaris luput dari perhatian publik, bisnis VC yang menjadi salah satu

memastikan startup yang akan menerima pendanaan di masa depan bisa mendapatkan dukungan *know how* untuk bisa tumbuh dengan baik.

Cara Baru Dekatkan Investor dan Startup

Adalah Alpha Momentum – perusahaan VC yang berani melakukan terobosan melalui penyelenggaraan sebuah event berskala besar. Tidak seperti event pada umumnya, Alpha Momentum mendesainnya sebagai sebuah platform bertemunya semua pelaku dalam ekosistem startup mulai para VC, venture capitalis atau investor, praktisi berbagai industri, dan startup.

Alpha Momentum adalah VC yang didirikan oleh para pelaku industri TIK dari berbagai negara dengan latar belakang berbeda, mulai veteran dari perusahaan yang masuk Fortune 500, founder startup hingga IT Solution Provider yang memiliki jaringan kuat dengan para praktisi dan pakar di bidang teknologi terkini seperti *blockchain*, *artificial intelligence*, *big data*, *internet of things*, *virtual reality* hingga *augmended reality*.

Kelvin Yim executive director & founding mentor Alpha Momentum menjelaskan pendekatan baru yang dilakukan perusahaannya dan optimismenya terkait penyelenggaraan event Starthub Connect yang akan mendorong perubahan cara berinvestasi dan pengembangan startup di Indonesia. "Melalui event ini semua yang terlibat dalam ekosistem startup dapat bertemu langsung. Para investor dan startup juga seringkali menanyakan berbagai hal yang tidak bisa kami jawab dengan pasti dan mereka bisa dengan cepat memperolehnya di event ini. Ini merupakan cara baru yang lebih efektif dan produktif bagi semua pelaku industri ini."

Membangun Platform untuk VC dan Startup

Kelvin mengungkapkan pihaknya memiliki rencana jangka panjang dan tidak hanya untuk mengubah cara bagaimana investor berinvestasi dan juga sebaliknya bagaimana startup mencari investor dan mengembangkan bisnisnya. Melalui StartHub Connect, Alpha Momentum bertujuan menyediakan sarana bagi seluruh pemain dalam ekosistem startup di Indonesia meraih kesuksesan di masa depan. Sudah menjadi pengetahuan bersama bahwa tingkat kesuksesan startup di Indonesia masih sangat rendah dan ini tentu juga merugikan bagi para VC, investor dan perekonomian Indonesia secara umum.

" Menteri Komunikasi dan Informatika, Rudiantara pernah mengatakan bahwa tingkat kesuksesan startup di Indonesia baru mencapai tiga persen. Hal ini membutuhkan perhatian yang serius dari berbagai pihak. Selama ini baik VC maupun startup di Indonesia lebih banyak mengandalkan jaringan pertemanan untuk membangun jaringan atau menyalurkan dan mendapatkan *funding*. Belum tersedia platform terstuktur yang memungkinkan kedua belah pihak untuk bertemu sehingga bisa secara lebih obyektif saling menemukan mitra yang tepat baik VC untuk mengetahui lebih banyak startup maupun startup untuk menemukan VC yang memiliki komitmen jangka panjang bagi keberlanjutan bisnisnya.

Dengan latar belakang inilah, Kelvin menjelaskan mengapa Alpha Momentum membangun platform yang memungkinkan semua yang terkait dengan ekosistem startup di Indonesia dapat bertemu dan berinteraksi secara lebih efektif dan produktif. Dengan jaringan nasional dan internasional yang dimilikinya, Alpha Momentum akan memfasilitasi investor maupun startup di Indonesia untuk bisa saling lebih mengenal dan melakukan penjajagan untuk selanjutnya membangun kolaborasi.

"Kami memiliki komitmen untuk mendorong kesuksesan startup seperti saat kami membangun perusahaan dimana kami bekerja selama ini. Pertanyaan yang selalu kami tekankan untuk mendorong kinerja kami adalah bagaimana kami bisa terus mengembangkan jaringan untuk mengembangkan perusahaan kami di masa lalu. Kami ingin menjadi katalis bagi investor dan startup di Indonesia. Dan kami meyakini cara baru yang kami tawarkan ini tepat dan memang dibutuhkan baik oleh para investor dari berbagai industri maupun negara maupun startup Indonesia."



iCIO COMMUNITY



Background

The iCIO Community is an Indonesian community of senior IT leaders and decision makers who come together to share their experience, knowledge and wisdom.

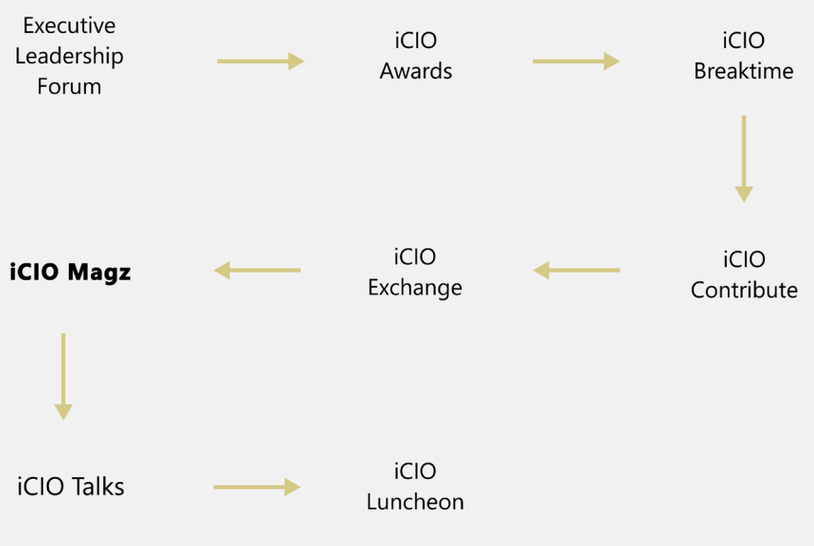
Our Purpose

Become a premiere community of IT leaders and decision makers that provides the trusted knowledge, resources *peer-to-peer* collaboration to enable you to become a more effective leader, driving personal and organizational result.

Our Mission

The iCIO Community is a community with the resources, expertise, and credibility required to help you meet a wide range of goals - shorts and long-term, individual and collective. Provide a profesional community that connects you with targeted professional networks, valued information, trusted organizations, and innovative discussions.

Our Programs





THE BOARD OF COMMITTEE

CHAIRMAN

Rico Usthavia Frans
Director of IT & Operation
PT. Bank Mandiri Tbk.

SECRETARY GENERAL

Jeny Musthopa
Chief of Information Technology
Services Commonwealth Life

TREASURER

Dickie Widjaja
Chief Information Officer,
Investree

EXECUTIVE DIRECTOR

Rachmat Gunawan
Director of CTI Group

COORDINATOR DIVISION

MEMBERSHIP

Debbie Nova
Group Chief Information Officer Coca-Cola Amatil

YB. Hariantono
Direktur Operation & IT,
PT. Bank Mega Tbk

Dewi T. Saleh
IT Director PT. Kawan Lama Sejahtera

PARTNERSHIP

Novaldy Antonio
Senior Manager Information Technology Services RSPI

Ivan Sangkereng
IT Director Bina Nusantara Group

RESEARCH

Hermawan Thendean
Executive Vice President
PT. Bank Central Asia Tbk

Abidin Riyadi Abie
IT & GA Division Head
PT Toyota Astra Financial Services

COMMUNICATION

Danny Natalies
CIO Universitas Katolik Atmajaya, Jakarta

Lukas Djuanda
CIO PT. Japfa Comfeed Indonesia Tbk

ADVOCACY

Jean H. Reksodiputro
CIO PT. Pefindo Credit Bureau

Achmad Royhan
Vice President Information Technology PT. Citilink Indonesia

BOARD OF ADVISORY



Harry Surjanto
President Director of
CTI Group



Agus Wicaksono
CIO Chevron Indonesia



Ongki Kurniawan
Managing Director GrabPay
Indonesia



M. Kuncoro Wibowo
Staff Ahli, Kementrian Energi
dan Sumber Daya Mineral



Adikin Basirun
Independent Commisioner,
PT. UOB Kay Hian Securities



Dino Bramanto
Corporate IT Director

PROGRAMS

/prō.gram/



EXECUTIVE LEADERSHIP FORUM

CIO dan para pemimpin bisnis lainnya seperti CEO, CMO, CFO seringkali memiliki agenda yang berbeda-beda terkait dengan TI. Konsentrasi CIO biasanya pada hal-hal yang bersifat operasional, sementara CEO fokus pada strategi untuk mendorong pertumbuhan organisasi, CFO pada keuangan dan CMO pada bagaimana meningkatkan pengalaman pelanggan. Perbedaan cara pandang ini harus diminimalisasi agar TI bisa menjadi enabler untuk kinerja perusahaan yang lebih baik. iCIO Executive Leadership Forum didesain untuk menjawab tantangan yang dihadapi para executive bisnis ini.





iCIO TALK

iCIO Talk merupakan sarana untuk mempermudah CIO dan pemimpin bisnis lainnya untuk berbagi berbagai praktik bisnis terbaik yang terkait dengan TI. iCIO Community akan memfasilitasi mereka melalui wawancara untuk kemudian dipublikasikan dalam bentuk video maupun artikel.



iCIO EXCHANGE

Memberikan Anda kesempatan untuk berbagi kepada rekan-rekan CIO bagaimana lingkungan kerja Anda yang menantang. Program ini mengakomodasi anggota untuk bertemu dan berbagi pandangan tentang lingkungan kerja lintas industri.



iCIO CONTRIBUTE

iCIO Contribute merupakan gerakan para CIO ke Universitas dan lembaga pendidikan tinggi untuk berbagi cerita dan memotivasi mahasiswa melalui kegiatan mentorship, berbagi pengetahuan pengetahuan teknis dan pengalaman kerja. Tujuan program ini adalah untuk mendukung program-program dari lembaga pendidikan tinggi dalam mendekatkan dunia pendidikan dengan dunia kerja yang sesungguhnya.

iCIO AWARDS

iCIO Awards adalah penghargaan yang diberikan kepada para CIO dan staf senior di bidang TI yang telah terbukti sukses menghadirkan nilai terbaik dari TI di lingkungan organisasi. Penghargaan tahunan ini ditunjukan untuk memberikan motivasi dan mendorong para CIO untuk terus menigkatkan kinerja dan prestasinya sehingga pemanfaatan TI dapat memberikan kontribusi positif bagi pertumbuhan organisasi secara berkela



iCIO BREAKTIME

iCIO Breaktime adalah sebuah program yang didesain untuk menyediakan waktu dan ruangan bagi para CIO untuk bersantai sejenak dari tekanan pekerjaan sehari-hari. Para CIO dapat bersantai dengan peer group-nya sambil berbagi pengalaman dan berbincang seputar dunia mereka sembari melakukan hobinya.



TECHNOLOGY CENTER

Our Technology Center provides the latest technology in heterogeneous platform as a showcase of IT Infrastructure Laboratory. Members may utilize the Technology Center in all possible simulation ways for Proof of Concept, Trouble Shooting, and Porting Purposes.





WHY BECOME MEMBER?

Anggota akan bergabung dalam sebuah komunitas CIO dan staf senior di bidang TI dan ahli yang akan berbagi pengalaman, pengetahuan hingga berbagai praktik terbaik dibidang TI sehingga bisa membantunya menjadi pemimpin yang lebih efektif.

iCIO Community ditunjukan untuk menjadi sebuah platform yang dapat menjadi sarana bagi anggotanya untuk berinteraksi dengan sesama dan berbagai pihak terkait yang relevan, sehingga dapat membantu para member memperkaya pengetahuan yang diperlukannya dalam memimpin organisasi maupun pengembangan diri secara personal sebagai professional.

iCIO Community juga didukung oleh fasilitas Technology Center yang memungkinkan para anggotanya melakukan berbagai simulasi untuk proof of concept, trouble shooting dan porting sehingga mempermudah sharing pengetahuan dan pengalaman secara teknis. iCIO Community dikelola secara demokratis dan transparan dijalankan oleh komite yang akan berinteraksi dengan para anggotanya.

Begitu menjadi anggota, Anda dapat terlibat langsung dalam pengembangan komunitas ini maupun berbagai aktivitas yang telah ada sesuai dengan ketersediaan waktu dan keinginan anda.

iCIO Community juga mengajak para anggota, untuk mendorong para CIO atau pemimpin bisnis lain bergabung dalam komunitas ini sehingga tujuan dari komunitas ini untuk menjadi platform bagi para anggotanya untuk menjadi pemimpin yang lebih efektif dan pengembangan diri secara personal sebagai profesional dapat tercapai.



CONNECT WITH US

- iCIO Community
- Committee of iCIO Community
- iCIO Community
- www.ciocommunity.org
- monthly e-newspaper
- quarterly iCIO Magz

iCIO
COMMUNITY

TERIMA KASIH

atas dukungan dan kontribusi terhadap
Perkumpulan Chief Information Officer Indonesia
Tahun 2016-2018



Ongki Kurniawan | Iskak Hendrawan | Lukas Djuanda | Adikin Basirun | Rachmat Gunawan | Jeny Mustopha | Agus Wicaksono | Debbie Nova | Harry Surjanto | Jean H. Reksodiputro | Ivan Sangkereng | Novaldy Antonio | Dino Bramanto

iCIO COMMUNITY

Traveler 2018



Alibaba Cloud: THE COMPUTING CONFERENCE

Hangzhou, China

18th - 23rd Sept 2018

"It's ***not the technology*** that changes the world, It's ***the dream behind the technology*** that changes the world."

- JACK MA, Executive Chairman of Alibaba Group -

AGENDA

- 3 Days of **Alibaba Cloud Conference**
- Tour to **Alibaba Headquarters & Alibaba Xixi Campus**
- Visit to several sites with **Alibaba Technology Implementation**
- **Sightseeing** around Hangzhou

RSVP : committee@ciocommunity.org
*Registration Only for iCIO Member