IMFBlog
INSIGHTS AND ANALYSIS ON ECONOMICS & FINANCE

Memprakirakan Risiko *Cyber* untuk Sektor Keuangan

Oleh Christine Lagarde

22 Juni 2018

Rata-rata kerugian tahunan lembaga keuangan dari serangan *cyber* bisa mencapai hingga ratusan miliar dolar per tahunnya. (foto: EtiAmmos/iStock oleh Getty Images)

Risiko *cyber* telah menjadi ancaman yang signifikan terhadap sistem keuangan. Sebuah pemodelan staf IMF memprakirakan bahwa rata-rata kerugian tahunan lembaga keuangan akibat serangan *cyber* bisa mencapai hingga ratusan miliar dolar per tahunnya, yang menggerus keuntungan bank dan berpotensi mengancam stabilitas keuangan.

Kasus-kasus terbaru menunjukkan bahwa ancaman tersebut nyata. Serangan yang berhasil dilakukan telah menghasilkan peretasan data di mana para pencuri memperoleh akses ke informasi rahasia dan penipuan, seperti pencurian $500 juta

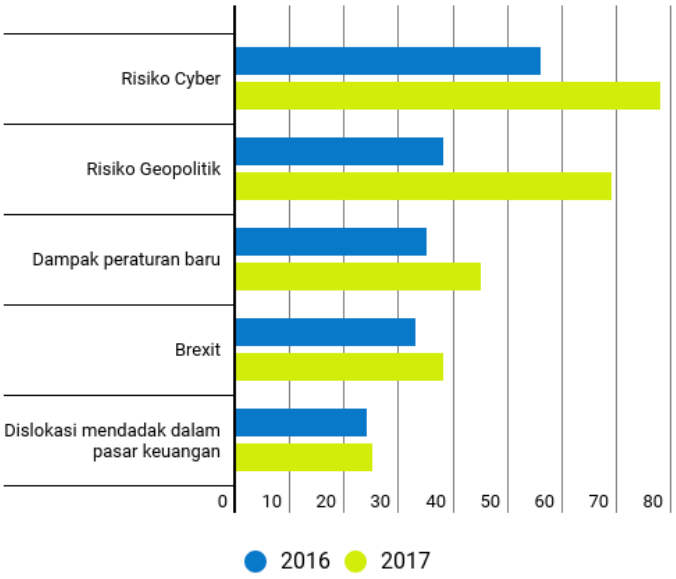
dari perusahaan penukaran mata uang *crypto* Coincheck. Dan terdapat ancaman bahwa lembaga yang ditargetkan mungkin tidak dapat lagi beroperasi.

Tidak mengejutkan, jika survei secara konsisten menunjukkan bahwa manajer risiko dan eksekutif lainnya di lembaga keuangan paling mengkhawatirkan terjadinya serangan *cyber*, seperti terlihat pada grafik di bawah ini.

Survei menempatkan risiko *cyber* di peringkat atas

Manajer risiko dan eksekutif keuangan lainnya melihat adanya ancaman serangan *cyber* yang semakin meluas, yang menghadirkan risiko lebih besar dibandingkan berbagai kejadian geopolitik dan peraturan baru.

(persen responden)



Sumber: Survei oleh Depository Trust & Clearing Corp., dipublikasikan sebagai DTCC Systemic Risk Barometer 2017Q1

INTERNATIONAL MONETARY FUND

Kerentanan sektor keuangan

Sektor keuangan terutama sangat rentan terhadap serangan *cyber*. Lembaga-lembaga keuangan tersebut merupakan target yang menarik karena peran penting mereka

dalam intermediasi dana. Suatu serangan *cyber* yang sukses pada satu lembaga dapat menyebar dengan cepat melalui sistem keuangan yang sangat saling terkoneksi. Berbagai lembaga masih menggunakan sistem lama yang mungkin tidak kuat menghadapi serangan *cyber*. Dan suatu serangan *cyber* yang sukses dapat memiliki konsekuensi langsung yang besar berupa kerugian finansial serta biaya tidak langsung, seperti reputasi yang menurun.

Kasus-kasus besar baru-baru ini semakin banyak menempatkan risiko *cyber* dalam agenda sektor resmi—termasuk berbagai organisasi internasional. Namun, analisis kuantitatif terkait risiko *cyber* masih berada pada tahap dini, terutama karena kurangnya data tentang kerugian akibat serangan *cyber*, dan berbagai kesulitan dalam pemodelan risiko *cyber*.

Sebuah studi terbaru IMF memberikan rerangka untuk memikirkan potensi kerugian akibat serangan *cyber* dengan fokus pada sektor keuangan.

Memprakirakan potensi kerugian

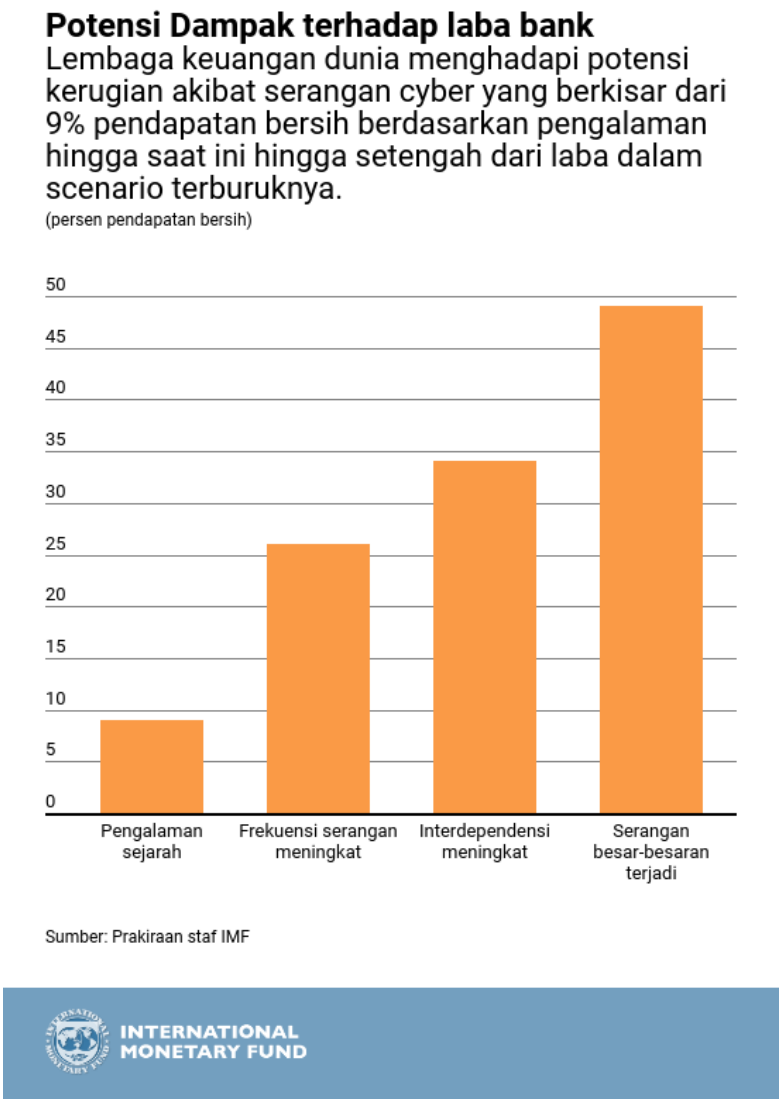
Rerangka pemodelan tersebut menggunakan teknik dari ilmu aktuaria dan pengukuran risiko operasional untuk memprakirakan kerugian agregat dari serangan *cyber*. Hal ini membutuhkan pengukuran frekuensi serangan *cyber* terhadap lembaga keuangan dan suatu gambaran distribusi kerugian dari kejadian semacam itu. Simulasi numerik kemudian dapat digunakan untuk memprakirakan distribusi kerugian serangan *cyber* secara agregat.

Kami menjelaskan rerangka kami menggunakan kumpulan data yang mencakup kerugian baru-baru ini akibat serangan *cyber* di 50 negara. Di sini diberikan contoh bagaimana potensi kerugian bagi lembaga keuangan dapat diprakirakan. Upaya ini sulit dan menjadi lebih menantang karena data tentang risiko *cyber* amat kurang. Kemudian juga, beruntungnya, belum ada serangan *cyber* berskala besar yang berhasil dilakukan pada sistem keuangan.

Dengan demikian hasil-hasil perhitungan kami harus dianggap sebagai ilustratif. Dilihat sekilas, hasil perhitungan tersebut menunjukkan bahwa rata-rata potensi kerugian tahunan dari serangan *cyber* bisa besar, hampir 9 persen dari pendapatan bersih bank secara global, atau sekitar $100 miliar. Dalam skenario yang parah—di mana frekuensi serangan *cyber* bisa dua kali lebih tinggi daripada sebelumnya dengan persebaran yang lebih besar—kerugian bisa menjadi 2½ - 3½ kali lebih tinggi dari ini, atau sebesar $270 miliar hingga $350 miliar.

Rerangka ini dapat digunakan untuk mengkaji skenario risiko ekstrem yang melibatkan serangan besar-besaran. Distribusi data yang kami kumpulkan menunjukkan bahwa dalam skenario seperti itu, yang mewakili 5 persen kasus

terburuk, rata-rata potensi kerugian dapat mencapai setinggi setengah dari pendapatan bersih bank, sehingga menempatkan risiko pada sektor keuangan.



Prakiraan kerugian tersebut beberapa kali lipat lebih besar daripada ukuran pasar asuransi *cyber* saat ini. Meskipun dengan pertumbuhan baru-baru ini, pasar asuransi untuk risiko *cyber* tetap kecil, sekitar $3 miliar dalam bentuk premi global pada tahun 2017. Sebagian besar lembaga keuangan bahkan tidak memiliki asuransi *cyber*. Cakupannya terbatas, dan perusahaan asuransi menghadapi tantangan dalam mengevaluasi risiko karena ketidakpastian tentang paparan *cyber*, kurangnya data, dan kemungkinan efek persebaran.

Langkah ke depan

Terdapat banyak peluang untuk meningkatkan penilaian risiko. Pengumpulan data yang lebih rinci, konsisten, dan lengkap oleh pemerintah tentang frekuensi dan dampak serangan *cyber* akan membantu dalam menilai risiko bagi sektor keuangan. Persyaratan untuk melaporkan peretasan—seperti yang dipertimbangkan menurut Peraturan Perlindungan Data Umum milik Uni Eropa—dapat meningkatkan pengetahuan tentang serangan *cyber*. Analisis skenario dapat digunakan untuk mengembangkan penilaian komprehensif tentang bagaimana serangan *cyber* dapat menyebar dan merancang tanggapan yang memadai oleh lembaga-lembaga swasta dan pemerintah.

Kerja lebih lanjut diperlukan juga untuk memahami bagaimana memperkuat ketahanan lembaga keuangan dan infrastruktur, baik untuk mengurangi peluang serangan *cyber* yang sukses maupun juga untuk memfasilitasi pemulihan yang lancar dan cepat. Ada juga kebutuhan untuk membangun kapasitas di sektor resmi di banyak bagian dunia untuk memantau dan mengatur risiko-risiko tersebut.

Singkatnya, diperlukan penguatan rerangka regulasi dan pengawasan untuk risiko *cyber*, dan berbagai upaya harus fokus pada praktik pengawasan yang efektif, pengujian kerentanan dan pemulihan yang realistis, dan perencanaan kontinjensi. IMF memberikan bantuan teknis untuk membantu negara-negara anggota memperbaiki rerangka regulasi dan pengawasan mereka.

*****

Christine Lagarde adalah Direktur Pelaksana Dana Moneter Internasional. Setelah menjabat periode lima tahun pertamanya, beliau kembali ditunjuk pada bulan Juli 2016 untuk masa jabatan kedua. Beliau adalah warga negara Prancis yang sebelumnya adalah Menteri Keuangan Prancis dari bulan Juni 2007 hingga Juli 2011, dan juga pernah menjabat sebagai Menteri Negara Perdagangan Luar Negeri Prancis selama dua tahun.

Christine Lagarde juga memiliki karir panjang dan penting sebagai pengacara anti-monopoli dan tenaga kerja, menjadi partner pada firma hukum internasional Baker & McKenzie, di mana ia dipilih sebagai ketua pada bulan Oktober 1999. Beliau memegang posisi tertinggi di firma hukum tersebut hingga bulan Juni 2005 ketika ia ditunjuk untuk jabatan pertamanya sebagai menteri di Prancis. Christine Lagarde memegang gelar dari Institute of Political Sciences (IEP) dan dari Fakultas Hukum Universitas Paris X, di mana beliau juga mengajar sebelum bergabung dengan Baker & McKenzie pada tahun 1981.

Buka di sini untuk bio lebih lengkap.

Tautan yang berhubungan:

Pertahanan *Cyber* Harus Global