IIA Bulletin

*Perspektif untuk auditor internal tentang masalah paling mendesak saat ini*

*Februari 2020*

# MEMIKIRKAN KEMBALI KESIAPSIAGAAN: PANDEMIK DAN *CYBERSECURITY*

**Epidemi *coronavirus* membawa pada fokus yang tajam** mengenai suatu masalah yang sering diabaikan oleh organisasi-organisasi — kesinambungan bisnis dan kesiapsiagaan bencana.


Ketidakpastian tentang ruang lingkup dan durasi epidemi ini telah berdampak, mulai dari organisasi mengevaluasi kembali rencana perjalanan karyawan sampai investor yang gelisah menjual sahamnya. Dengan potensi untuk mempengaruhi rantai pasokan, produktivitas pekerja, dan hubungan dengan pihak ketiga, risiko wabah yang meluas ini harus dipikirkan oleh para eksekutif bisnis dan pemimpin audit internal. Paling tidak, pimpinan audit internal harus siap untuk meninjau dan merekomendasikan pembaruan yang diperlukan untuk pandemi, kesiapsiagaan bencana, dan rencana kesinambungan bisnis.

Bahkan ketika organisasi berada pada tahap pertama dalam menentukan dampak potensial dari virus corona tehadap operasi organisasi, risiko tambahan muncul — rekayasa sosial di tengah krisis. Para penjahat dunia maya mengambil keuntungan dari kekhawatiran yang berkembang atas virus mematikan itu. Surat elektronik (surel) yang mengandung *malware* yang seolah-olah memberikan petunjuk tentang virus muncul di tiga prefektur Jepang, menurut TechRadar Pro, sebuah situs berita dan ulasan teknologi konsumen yang berbasis di Inggris. Peretas menyamarkan *malware* dalam lampiran surel yang mengaku berisi informasi untuk melindungi diri dari penyebaran virus. Sebaliknya, lampiran surel ini sarat dengan virus jenis lain, menurut TechRadar Pro.

Para penjahat dunia maya mengambil keuntungan dari krisis adalah sesuatu yang kemungkinan akan menjadi semakin umum. Organisasi harus membangun protokol dan praktik untuk bertahan melawan rekayasa sosial seperti *phishing*, *pretexting*, dan *baiting*.

## Pertanyaan umum untuk menilai kesiapsiagaan bencana organisasi Anda

**Berikut ini adalah beberapa pertanyaan umum** yang harus ditanyakan oleh departemen audit internal anda untuk menentukan apakah organisasi anda menangani kesiapsiagaan bencana dan perencanaan kesinambungan bisnis dengan tepat:

- Kapan terakhir kali rencana ketahanan organisasi ditinjau oleh pemangku kepentingan utama? Kapan terakhir kali rencana organisasi diuji dan oleh siapa?
- Bagaimana rencana terkini organisasi dalam menangani bencana alam, pandemi, atau gangguan potensial lainnya yang dapat memengaruhi fasilitas ? Karyawan anda? Penyedia *cloud* anda? Pemasok anda? Pelanggan anda?
- Kapan terakhir kali organisasi meninjau kontrak dengan mitra ketahanan bisnis?
- Bagaimana vendor, responden darurat, regulator, agen asuransi, dan pemangku kepentingan penting lainnya diberitahu tentang perubahan kontak?
- Seberapa mampukah organisasi untuk melakukan versi manual dari aktivitas otomatis yang penting untuk bisnis? Apakah formulir dan manual prosedur yang diperlukan tersedia? Apakah anda memiliki staf yang tepat untuk melakukannya?
- Seberapa sering organisasi memverifikasi kegentingan dari berbagai proses bisnis untuk memastikan urutan pemulihan sudah tepat? Bagaimana TI memastikan komponen infrastruktur penting telah diaktifkan untuk memungkinkan persyaratan pemulihan bisnis?
- Sasaran bisnis apa yang akan terhambat atau tertahan jika akses internet atau seluler terbatas atau tidak ada?
- Pelatihan apa yang telah diterima karyawan dan rekan bisnis tentang apa yang harus dilakukan jika terjadi bencana alam atau pandemi?
- Apakah pusat data dan/atau penyedia *cloud* mampu menjalankan "lampu padam," yang berarti tidak ada pekerja yang hadir dalam waktu lama?
- Proses atau aktivitas bisnis penting apa yang tidak dapat ditransfer ke lokasi alternatif? Yang memiliki implikasi peraturan berdasarkan waktu atau durasi acara?

## Pertanyaan umum untuk menilai kerentanan rekayasa sosial organisasi

**Berikut ini adalah beberapa pertanyaan umum** yang harus ditanyakan oleh departemen audit internal Anda untuk menentukan kerentanan organisasi anda terhadap skema rekayasa sosial:

- Apa praktik, kebijakan, dan pelatihan organisasi yang melibatkan ancaman rekayasa sosial? Bagaimana hal-hal ini dikomunikasikan kepada karyawan dan diberlakukan?
- Apakah ancaman rekayasa sosial sepenuhnya dipahami dan dikomunikasikan kepada semua tingkat karyawan di organisasi?
- Sistem dan proses apa yang paling rentan terhadap rekayasa sosial? Proses bisnis utama apa yang berpotensi terpengaruh?
- Pengujian apa yang dilakukan departemen TI Anda yang berkaitan dengan bidang kerentanan spesifik terhadap rekayasa sosial?
- Apakah Anda memiliki rencana untuk mengaudit area kerentanan organisasi Anda terhadap rekayasa sosial?

# IIA RESOURCES

**Knowledge Brief**

- Strategic Public Asset Protection

**Practice Guides**

- Assessing the Risk Management Process
- Auditing Third-Party Risk Management
- Coordination and Reliance: Developing an Assurance Map
- Business Continuity Management
- GTAG: Business Continuity Management
- GTAG Assessing Cybersecurity Risks

**Internal Auditor magazine**

- In the Face of Nature

Diterjemahkan dan diselaraskan oleh IIA Indonesia Volunteer:

1. Diana Laurencia Sidauruk, S.E., M.Sc.
2. Subagio Tjahjono, SE, MM, CIA, CISA, CFE, CRISC, CPA, ASEAN CPA