# 2008 Tahunan Penilaian Komunikasi Google 2008

Buku putih Google
Februari 2008

Google™

# Ringkasan Eksekutif

Pada akhir tahun 2007, Google melakukan survei online tahunan tentang staf profesional sistem pesan. Memberikan informasi tentang tren komunikasi utama selama setahun terakhir dan menekankan masalah serta kekhawatiran tren komunikasi pada tahun yang akan datang, survei ini merupakan hasil wawancara global dengan 575 CEO, CIO, dan CTO di perusahaan multinasional besar dan organisasi kecil.

Laporan ini merangkum hasil penting survei tersebut, termasuk analisis statistik rinci tren utama dalam komunikasi bisnis pada tahun 2007 serta cara tren diterjemahkan menjadi prioritas bagi staf profesional komunikasi bisnis di tahun mendatang. Mengacu pada ringkasan hasil penelitian, laporan tersebut memenuhi harapan Google pada tahun berikutnya dan menjelaskan beberapa penerapan terbaik dalam komunikasi bisnis untuk membantu organisasi menjawab tantangan industri pada tahun 2008.

## Hasil penting

### 1. Jumlah pesan elektronik meningkat pada tahun 2007 dan spam masih menjadi masalah besar bagi sebagian besar organisasi

Komunikasi elektronik − email, Web, dan IM (pesan cepat) − terus berkembang secara nyata pada tahun 2007, disertai peningkatan nyata volume spam. Berdasarkan data dari pusat data Postini (Postini, Inc. adalah anak perusahaan yang dimiliki sepenuhnya oleh Google Inc.), volume spam per pengguna meningkat 57% pada tahun 2007 dibandingkan pada tahun 2006. Apakah artinya? Hal tersebut berarti bahwa pengguna yang tidak dilindungi secara rata-rata menerima 36.000 pesan spam pada tahun 2007, dibandingkan dengan 23.000 pesan spam pada tahun 2006. Spam hingga saat ini masih menjadi masalah keamanan komunikasi teratas yang dihadapi perusahaan.

### 2. Eksekutif mengandalkan staf TI, bukan pengguna akhir, untuk memastikan keamanan dan kepatuhan

Menurut peserta survei ini, keamanan dan kepatuhan komunikasi sepenuhnya dibebankan kepada staf TI. Bahkan, 53% dari semua eksekutif dan profesional sistem pesan yang disurvei mengindikasikan bahwa mereka menganggap divisi TI adalah divisi yang paling bertanggung jawab atas keamanan dan kepatuhan komunikasi. Hanya 18% dari peserta survei merasa bahwa akuntabilitas keamanan dan kepatuhan merupakan tanggung jawab TI serta pengguna akhir.

### 3. Profesional TI menghadapi tantangan serius dalam mencapai tujuan keamanan dan kepatuhan

Responden memahami bahwa memastikan keamanan dan kepatuhan komunikasi bukan merupakan tugas yang mudah dan terdapat tantangan serius di kedua bidang tersebut. Dalam keamanan komunikasi, sebagian besar responden khawatir tentang perlindungan mereka terhadap spam, virus, dan worm; keamanan staf lapangan, kepastian akan ketersediaan serta kelanjutan bisnis; dan penanganan masalah tantangan tersebut pada sumber daya TI. Demikian juga tantangan besar yang dihadapi oleh organisasi dalam mencapai tujuan kepatuhan adalah perencanaan pemulihan kerugian, kepastian proses kepatuhan bisnis, pencegahan kebocoran data yang tidak disengaja, serta perlindungan sistem internal terhadap pelanggaran oleh hacker.

### 4. Tantangan keamanan dan kepatuhan berdampak negatif terhadap produktivitas TI

Pada akhir tahun 2007, eksekutif sangat khawatir tentang pengaruh keamanan dan kepatuhan komunikasi terhadap produktivitas TI. Waktu yang diperlukan dalam memastikan diterapkannya prosedur kepatuhan (46%), mengatur peningkatan

kemampuan sistem untuk meningkatkan keamanan (44%), dan mengatasi ketidaktersediaan atau penangguhan jaringan akibat pelanggaran keamanan (42%) memiliki nilai tinggi dalam daftar kekhawatiran responden.

**5. Solusi keamanan komunikasi dan kepatuhan berbasis model SaaS (Software-as-a-Service) dapat mengatasi masalah produktivitas tersebut**

Meskipun terdapat berbagai pendekatan untuk memastikan keamanan dan kepatuhan komunikasi, responden survei memahami bahwa manfaat solusi berbasis pendekatan Saas secara langsung mengatasi masalah produktivitas yang merupakan kekhawatiran terbesar, termasuk kemudahan penerapan, kemudahan pemeliharaan dan penanganan masalah, serta efektivitas solusi secara keseluruhan. Bahkan, 31% dari organisasi yang disurvei telah menggunakan beberapa jenis solusi SaaS karena manfaat yang diperoleh.

**6. Pada tahun berikutnya, Google mengharapkan jumlah ancaman tetap stabil, namun ternyata kerumitannya meningkat drastis**

Meskipun Google tidak mengharapkan jumlah ancaman keamanan komunikasi bisnis meningkat pesat pada tahun berikutnya, namun kami mengantisipasi peningkatan kerumitan ancaman tersebut. Perusahaan akan menghadapi tantangan untuk mengidentifikasi berbagai jenis konten berbahaya baru serta melindungi informasi yang sensitif dari teknik rekayasa sosial berkembang dan menghindari tindakan keamanan dengan memanipulasi atau menipu pengguna untuk mengungkapkan atau melakukan tindakan yang mengungkapkan data rahasia. Untuk menghindari kemungkinan kebocoran data, kami mengharapkan setiap organisasi untuk meningkatkan penekanan terhadap kebijakan keamanan keluar serta enskripsi konten pada tahun mendatang.

# Tren Komunikasi Bisnis tahun 2007

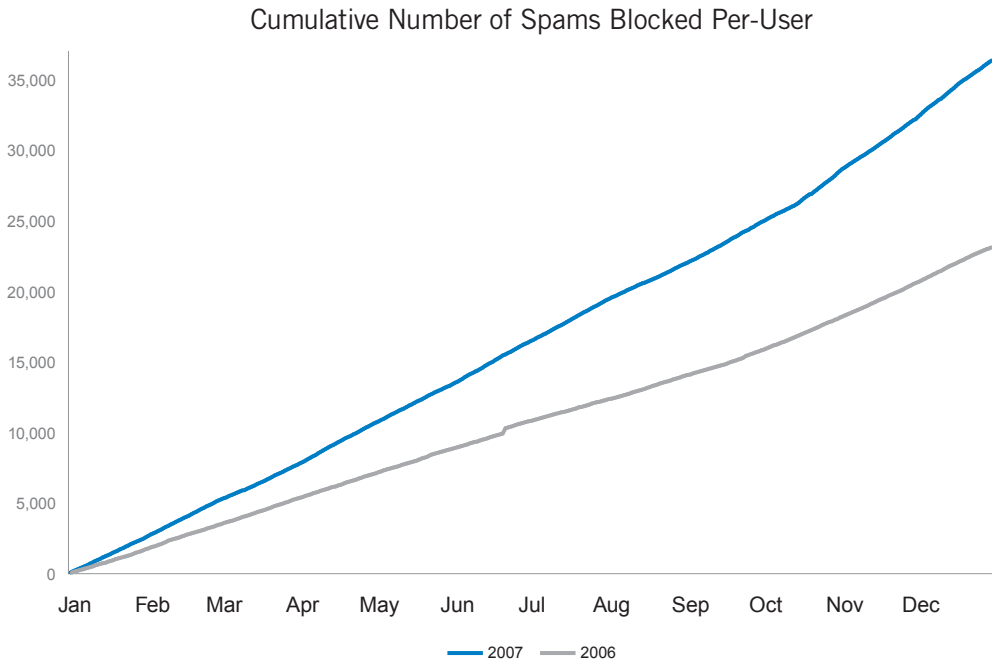
Survei online profesional dan eksekutif komunikasi bisnis Google mengungkapkan beberapa tren penting dalam komunikasi sepanjang tahun lalu. Survei eksekutif tersebut juga memberikan informasi tentang dampak tren tersebut terhadap prioritas utama pada tahun berikutnya. Berikut adalah bagian yang menjelaskan secara rinci hasil survei serta memberikan statistik pesan dari Postini, akuisisi Google terbaru.

**Tren #1: Karena jumlah pesan elektronik meningkat pada tahun 2007, spam masih menjadi masalah terbesar bagi sebagian besar organisasi**

Peningkatan komunikasi pada tahun 2007 − melalui email, Web, dan IM − sekaligus meningkatkan volume spam. Pada tahun 2007, pusat data Postini mencatat tingkat serangan spam dan virus tertinggi dalam sejarah. Sedangkan volume pesan email keseluruhan per pengguna meningkat sebesar 47% pada tahun 2007 dibandingkan tahun sebelumnya, volume spam meningkat sebesar 57% dalam jangka waktu yang sama, menurut penelitian pusat data Postini. Peningkatan tersebut dipicu oleh bertambahnya jumlah komputer bot-net − jaringan PC yang terinfeksi dengan koneksi Internet broadband − yang dilakukan oleh hacker tanpa sepengetahuan pemilik untuk mengirim pesan spam dan serangan virus.

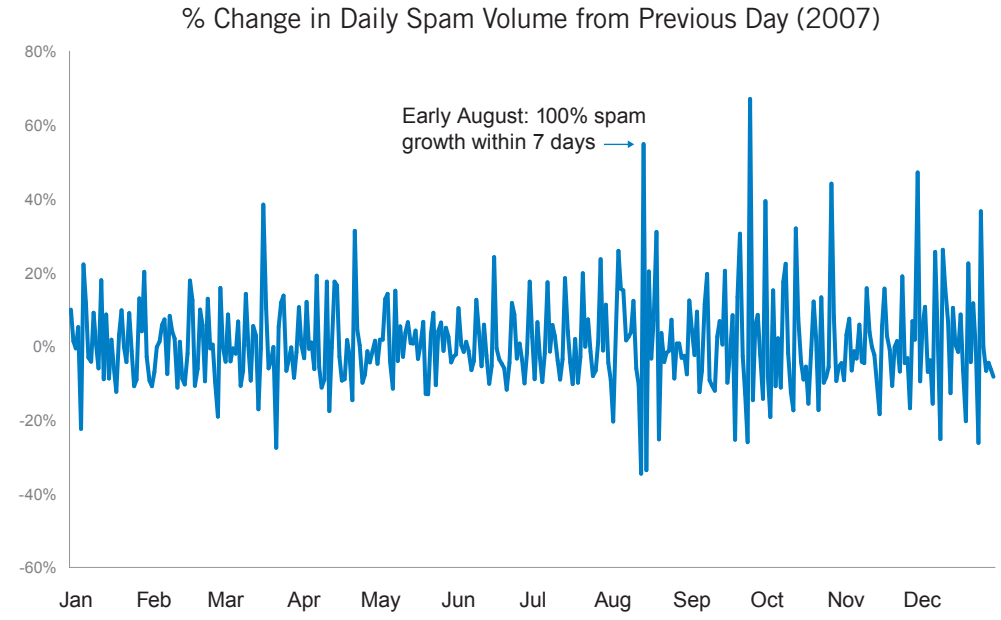
Pada tahun 2007, Postini memblokir 160% lebih banyak pesan spam dibandingkan pada tahun 2006, meskipun kecanggihan spammer juga bertambah dalam upaya menghindari deteksi oleh penyaring spam. Awal tahun 2007 ditandai dengan populernya spam gambar, yakni konten spam yang terdapat dalam gambar dan terlampir pada pesan email. Sepanjang tahun tersebut, spam gambar menurun dan digantikan oleh konten spam yang terdapat dalam PDF, dokumen, spreadsheet, dan bahkan lampiran multimedia, misalnya file MP3.

**Gambar 1**
Volume spam meningkat sebesar 57% dari tahun 2006 hingga 2007.
Sumber: Postini




Meskipun peningkatan volume spam serta inovasi dalam jenis ancaman spam secara keseluruhan membuat organisasi sangat khawatir, namun sebenarnya ketidakstabilan spam merupakan masalah yang lebih besar. Menurut penelitian pusat data Postini, volume rata-rata pesan spam per pengguna melonjak pada bulan Agustus 2007. Lonjakan tersebut bahkan mencapai 100% dalam waktu 7 hari. Sangat sulit bagi organisasi untuk merencanakan aktivitas tersebut.

**Gambar 2**
Ketidakstabilan peningkatan spam di pertengahan kedua tahun 2007.
Sumber: Postini




Hal yang lebih penting, namun tidak digambarkan secara jelas dalam grafik adalah bahwa peningkatan tidak dapat diperkirakan secara virtual yang berarti bahwa organisasi harus mempertahankan sejumlah besar kapasitas yang tidak digunakan

untuk secara proaktif bersiap menghadapi peningkatan tidak terduga atau terus meningkatkan bandwidth secara reaktif agar dapat mengimbangi peningkatan tidak terduga. Misalnya, jika organisasi memiliki tingkat bandwidth yang tepat untuk menangani volume spam-nya pada tanggal 1 Januari 2007, organisasi tersebut harus meningkatkan bandwidth sebesar 145% untuk menghadapi ketidakstabilan serta peningkatan sepanjang tahun tersebut.

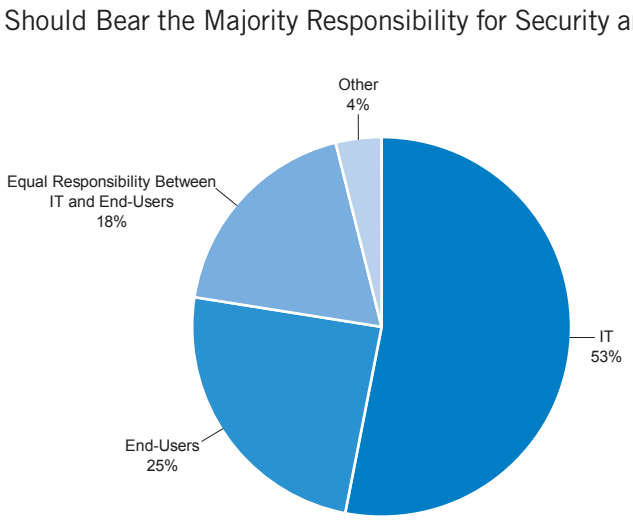
### Kesimpulan

Upaya dalam menghentikan spam dan bentuk malware lainnya masih menjadi prioritas bagi profesional komunikasi bisnis (48% responden menyebutnya sebagai kekhawatiran terbesar) karena peningkatan volume spam sebagai bagian dari semua komunikasi. Ketidakstabilan spam serta volume peningkatan tajam yang tidak dapat diperkirakan tersebut juga menambah tekanan di bidang keuangan bagi organisasi yang harus meningkatkan kapasitas untuk menghadapi ketidakpastian ini.

## Tren #2: Eksekutif mengandalkan staf TI, bukan pengguna akhir, untuk memastikan keamanan dan kepatuhan

Ketika ditanya tentang divisi yang paling bertanggung jawab atas keamanan dan kepatuhan komunikasi organisasi, jawaban sebagian besar responden survei online adalah divisi TI (53%). Hanya 25% yang merasa bahwa pengguna berkewajiban memastikan keamanan dan kepatuhan komunikasi elektronik. Hal yang menarik, 18% peserta survei merasa bahwa akuntabilitas keamanan serta kepatuhan merupakan tanggung jawab TI dan pengguna, dan 4% mengatakan bahwa divisi lainnya dalam perusahaan, seperti staf eksekutif, divisi hukum, bahkan personalia, berkewajiban menjaga keamanan serta kepatuhan komunikasi bisnis organisasi.

**Gambar 3**
Identifikasi responden terhadap tanggung jawab atas keamanan dan kepatuhan dalam organisasi.
Sumber: Penelitian Google




### Kesimpulan

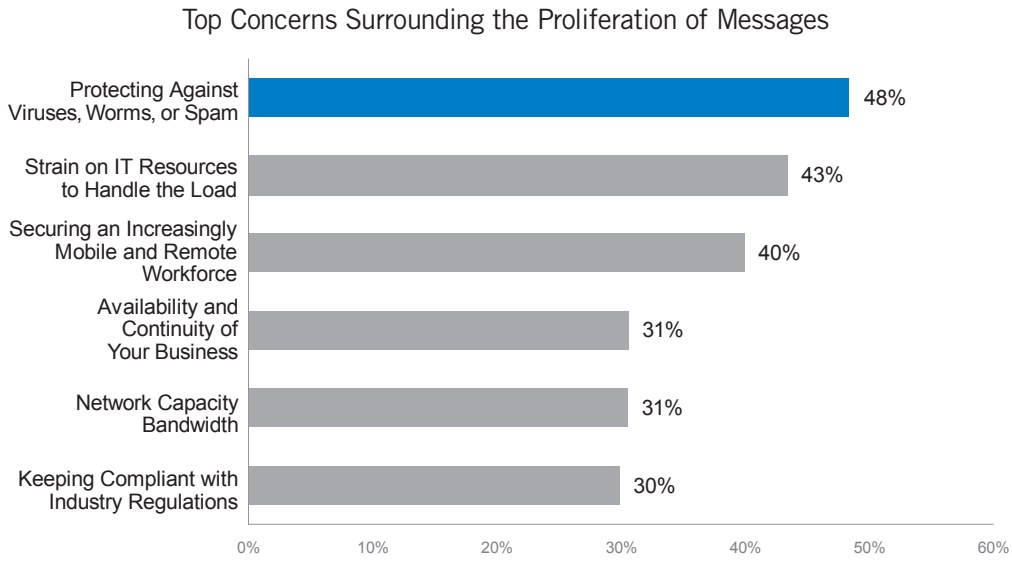
Seperti sebagian besar aspek keamanan dan kepatuhan peraturan perusahaan, divisi TI bertanggung atas keamanan dan kepatuhan komunikasi di sebagian besar perusahaan. Meskipun pengguna berperan dalam mewaspadai serta mempertahankan keamanan komunikasi dan kepastian kepatuhan, organisasi menyadari bahwa mereka harus memiliki mekanisme kebijakan untuk membantu pengguna menjaga keamanan dan kepatuhan.

### Tren #3: Profesional TI menghadapi tantangan serius dalam mencapai tujuan keamanan dan kepatuhan

Jumlah pesan elektronik yang terus meningkat disertai peningkatan spam, virus, worm, dan bahaya lainnya memberi tantangan nyata bagi organisasi dan divisi TI secara khusus dalam mencapai tujuan keamanan dan kepatuhan komunikasinya.

Pada sisi pengukuran keamanan, kekhawatiran terbesar di antara profesional sistem pesan adalah perlindungan organisasi terhadap ancaman tersebut (48% responden). Selain itu, eksekutif juga khawatir tentang cara sumber daya TI mengimbangi peningkatan pesat sistem pesan dan bahaya yang menyertainya (47%) serta cara mengamankan staf lapangan mereka (40%). Dengan mencermati data survei, responden dalam industri keuangan dan layanan kesehatan menyatakan bahwa kekurangan sumber daya TI menjadi kekhawatiran terbesar seputar manajemen pesan.

**Gambar 4**
Identifikasi responden terhadap kekhawatiran terbesar tentang peningkatan volume.
Sumber: Penelitian Google

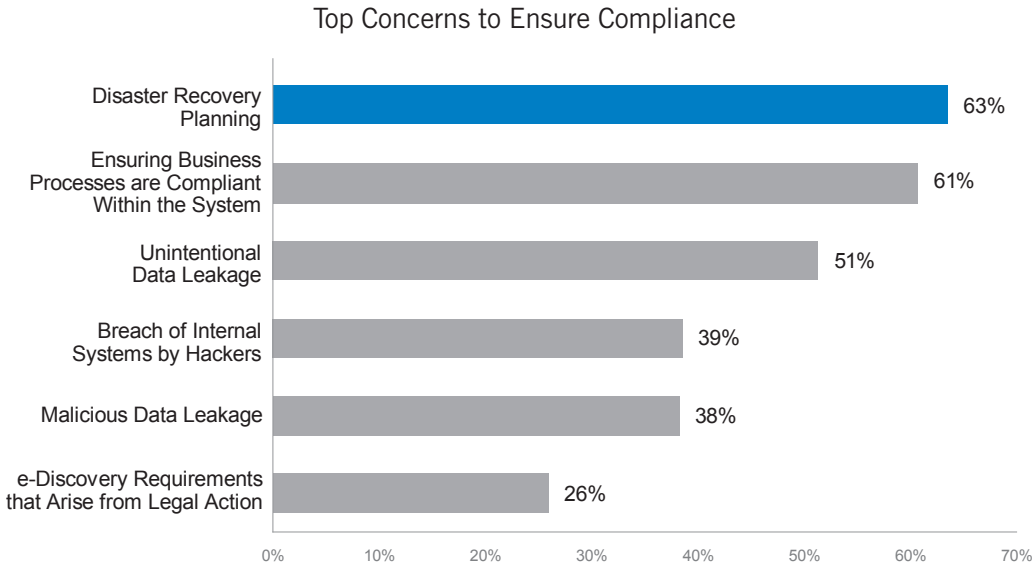



Memastikan kelanjutan bisnis jika terjadi masalah (misalnya, memulihkan data setelah kegagalan sistem yang besar, aksi teroris, atau bencana alam) serta mempertahankan kepatuhan proses bisnis dengan persyaratan peraturan yang terus berubah jelas merupakan masalah terpenting bagi organisasi yang berpartisipasi dalam survei ini, dengan 63% responden mengkhawatirkan pemulihan gangguan serta 61% berfokus pada kepastian kepatuhan proses bisnis. Hal yang menarik, perusahaan lebih khawatir tentang pengguna akhir yang secara tidak disengaja mengirim pesan berisi informasi rahasia atau kekayaan intelektual (51% responden) daripada pengguna akhir yang secara berbahaya melanggar keamanan dan kepatuhan perusahaan yang memberi tekanan lebih pada perusahaan TI untuk mencegah pelanggaran.

## Kesimpulan

Salah satu pemicu utama meningkatnya pesan adalah lonjakan jumlah jenis dan penggunaan teknologi selular. Setiap hari, pengguna menjadi lebih nyaman mengirim email dan IM serta menelusuri Web menggunakan laptop, ponsel, smart phone, dan perangkat selular lainnya. Semua komunikasi ini harus dianggap sebagai bagian dari rencana keamanan organisasi secara keseluruhan dan staf TI memahami peran mereka dalam menjaga keamanan komunikasi selular.

**Gambar 5**
Identifikasi responden terhadap kekhawatiran terbesar tentang kepatuhan pesan.
Sumber: Penelitian Google




Dengan memperhatikan kepatuhan, dampak hukum dan keuangan ketidaksesuaian terhadap peraturan merupakan masalah penting dan organisasi melakukan pendekatan yang lebih strategis dan proaktif untuk mempersiapkan diri. Dengan demikian, perusahaan membuat pengaturan kepatuhan yang dikepalai oleh COO (chief compliance officer) dan pengawasan dari kepala eksekutif. Hasilnya, Organisasi ini cenderung menghadapi tantangan dalam mempertahankan kepatuhan terhadap peraturan.

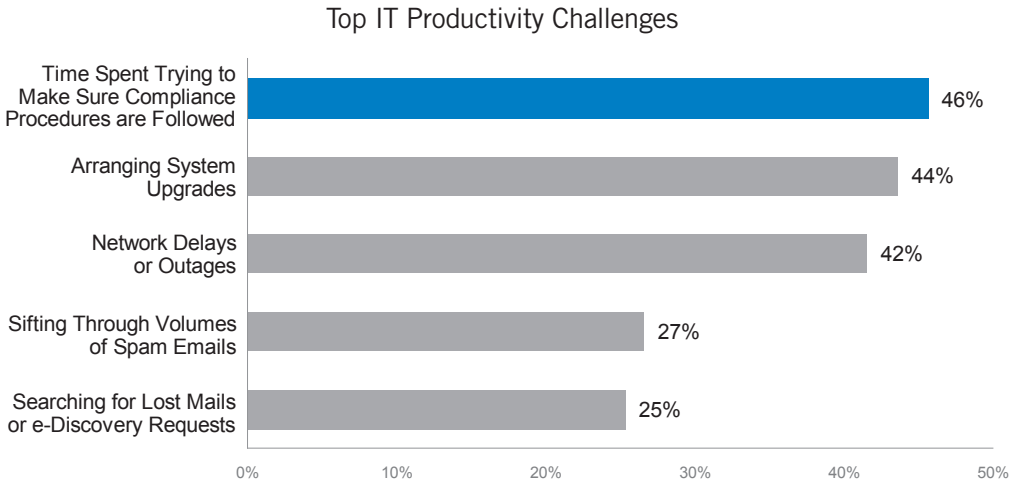
### Tren #4: Upaya memastikan keamanan dan kepatuhan komunikasi merupakan penurunan produktivitas yang nyata pada sumber daya TI

Responden survei setuju bahwa memastikan keamanan dan kepatuhan komunikasi mengakibatkan penurunan produktivitas yang nyata pada divisi TI mereka. Tiga penurunan produktivitas teratas pada staf TI yang disebutkan dalam survei mencakup memastikan diterapkannya prosedur kepatuhan (46%), mengatur peningkatan kemampuan sistem (44%), dan mengatasi ketidaktersediaan atau penangguhan jaringan (42%). Hal yang tidak terlalu sering diungkapkan, namun berdampak pada produktivitas adalah penyaringan email untuk menentukan legitimasi maupun bahayanya (27%) serta pencarian email yang hilang dan permintaan e-discovery lainnya (25%).

### Kesimpulan

Memastikan keamanan dan kepatuhan peningkatan jumlah pesan yang dikirim melalui beberapa saluran komunikasi bukan merupakan tugas yang mudah. Divisi TI di semua skala dan jenis perusahaan mendapatkan tugas tersebut yang pada tahap tertentu mereka tidak memiliki waktu untuk menggunakan aplikasi baru atau aktivitas bernilai tambah lainnya yang memiliki kontribusi pada penghasilan. Selanjutnya, organisasi harus mencari cara untuk mengurangi penurunan produktivitas akibat keamanan dan kepatuhan komunikasi agar dapat tetap bersaing.

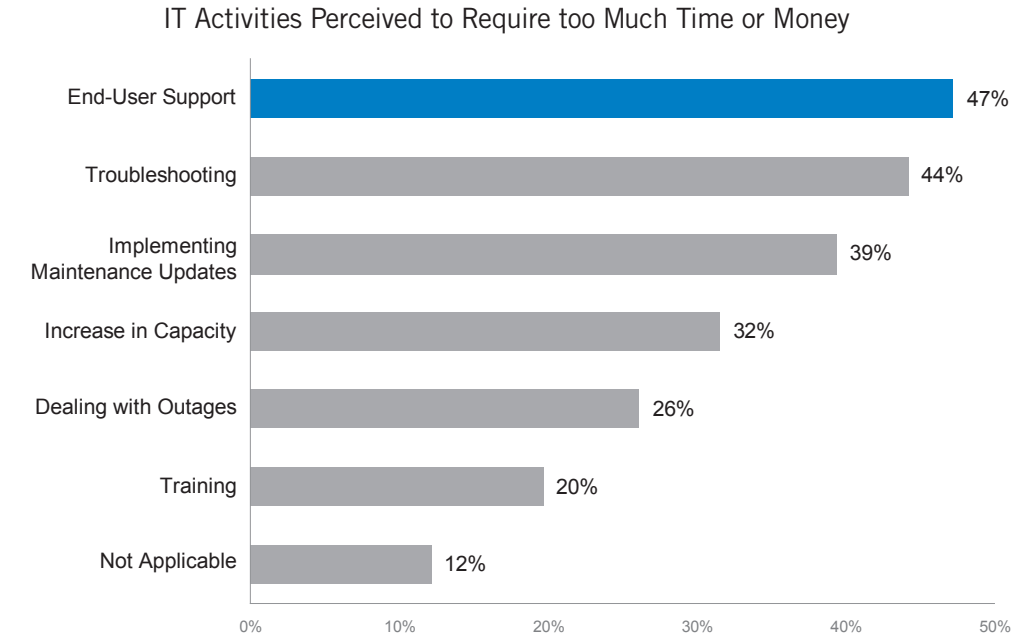
**Gambar 6**
Identifikasi responden terhadap tantangan utama seputar penurunan produktivitas TI.
Sumber: Penelitian Google




## Tren #5: Organisasi merasa menghabiskan terlalu banyak waktu dan biaya pada solusi keamanan dan kepatuhan saat ini serta memiliki beberapa persyaratan penting dalam daftar keinginan mereka untuk solusi yang mengatasi penurunan produktivitas dan keuangan tersebut

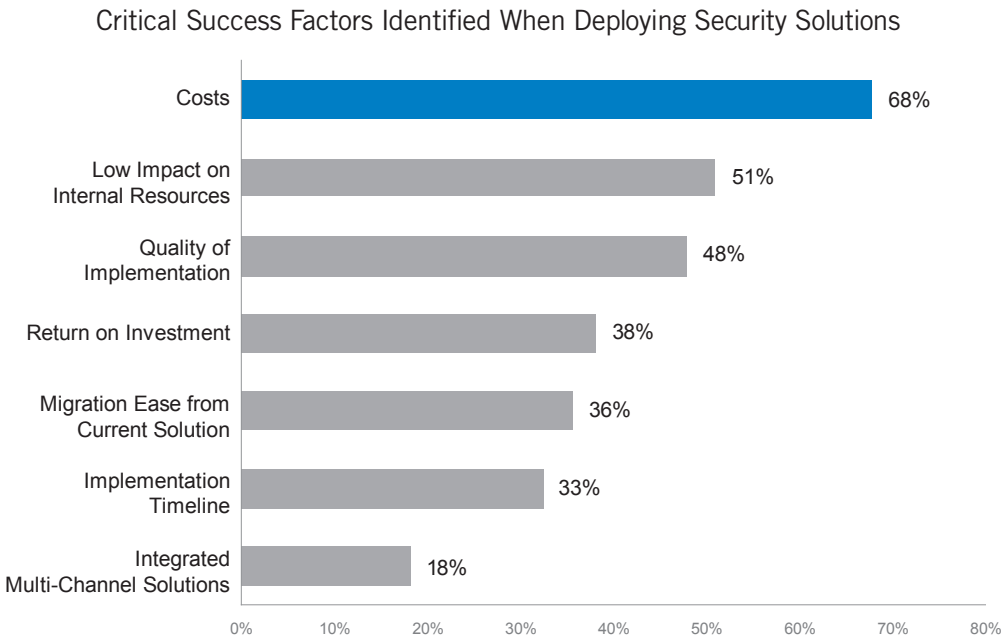
Saat ditanya tentang kepuasan terhadap solusi keamanan dan kepatuhan saat ini, hanya 12% responden survei online menjawab secara positif. Sebagian besar mengatakan bahwa mereka mereka menghabiskan terlalu banyak waktu dan biaya pada dukungan pengguna akhir (47%), mengatasi masalah (44%), menerapkan pembaruan pemeliharaan (39%), meningkatkan kapasitas (32%), dan menangani ketidaktersediaan (26%).

**Gambar 7**
Identifikasi responden terhadap area yang dianggap menghabiskan waktu dan biaya dalam solusi keamanan yang ada.
Sumber: Penelitian Google




Menggali lebih jauh lagi tentang fakta bahwa sangat sedikit responden yang puas terhadap solusi yang ada, Google meminta peserta mencantumkan kriteria utama dalam mengevaluasi serta menggunakan solusi keamanan dan kepatuhan komunikasi baru. Responden secara menyolok mengatakan biaya (68%) merupakan faktor utama yang dicari dalam solusi keamanan dan kepatuhan. Namun, kembali pada pada

**Gambar 8**
Identifikasi responden terhadap faktor penting keberhasilan saat menggunakan solusi keamanan.
Sumber: Penelitian Google




penurunan produktivitas yang disebabkan oleh banyak solusi saat ini, peserta survei juga menilai lebih solusi yang memiliki dampak kecil pada sumber daya internal (51%). Kualitas perangkat lunak (48%), laba atas investasi yang cepat (38%), serta migrasi yang mudah dari solusi saat ini (36%) juga disebutkan oleh responden survei sebagai kriteria penting dalam solusi keamanan dan kepatuhan komunikasi baru.

### Kesimpulan

Jelas bahwa organisasi khawatir tentang efektivitas solusi mereka saat ini dan sebagian besar perusahaan tidak menyukai status quo tersebut. Perusahaan TI menghabiskan terlalu banyak waktu dalam mengelola dan mempertahankan solusi keamanan dan kepatuhan komunikasi serta aktivitas dengan penghasilan yang tidak memadai, sehingga mempengaruhi penghasilan. Banyak perusahaan secara aktif mencari solusi baru yang akan mengurangi penurunan produktivitas TI, dapat digunakan dengan mudah dan cepat dalam organisasi, dan akan memberikan laba atas investasi yang cepat.

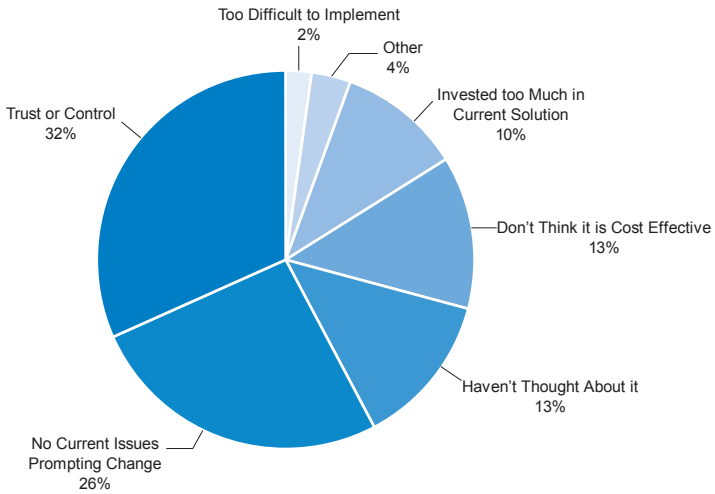
## Tren #6: Model SaaS sukses dalam popularitas dan pangsa pasar karena secara langsung mengatasi masalah produktivitas TI

Berkat pendekatan SaaS yang terbukti sukses dalam mengatasi masalah keuangan dan produktivitas penting yang umum dialami organisasi saat ini, sebagian besar responden survei sedang mengevaluasi atau telah menerapkan solusi SaaS. Hampir 31% organisasi yang disurvei menggunakan penyedia SaaS pada beberapa aspek infrastruktur teknologinya. Saat ditanya tentang alasan mereka memilih solusi SaaS, peserta survei menjawab persyaratan pemeliharaan dan penanganan masalah yang lebih sedikit (30%), kemudahan penerapan (23%), efektivitas secara keseluruhan (18%), dan biaya (12%) pendekatan SaaS. Responden mencantumkan manfaat yang sama saat ditanya tentang rangkaian keberhasilan penting pada penerapan keamanan yang membantu memahami alasan popularitas SaaS dalam industri TI.

**Gambar 9**
Identifikasi responden yang menggunakan solusi SaaS terhadap alasan mereka menyukai SaaS.
Sumber: Penelitian Google


Namun, tidak setiap orang yang disurvei tertarik dengan pendekatan SaaS. Dari 53% responden yang mengindikasikan bahwa mereka tidak menggunakan solusi SaaS, 32% mengatakan alasannya adalah ketidaknyamanan menyerahkan kontrol proses maupun fungsi tertentu kepada pihak eksternal. Menariknya, 26% mengatakan bahwa mereka tidak mengalami insiden tertentu yang memaksa untuk beralih ke solusi lainnya. Dan 17% dari semua responden sama sekali tidak memahami konsep SaaS.

**Gambar 10**
Alasan utama responden tidak menggunakan SaaS.
Sumber: Penelitian Google




Sedangkan 13% responden mengatakan bahwa mereka tidak menggunakan solusi SaaS karena tidak yakin tentang efektivitas biayanya, penelitian internal Google secara jelas mengilustrasikan keuntungan biaya pendekatan SaaS. Tabel berikut ini, berdasarkan penelitian, membandingkan perkiraan biaya solusi penyaringan email berbasis perangkat lunak atau perangkat dengan solusi berbasis SaaS dalam organisasi yang memiliki 1.000 karyawan pada umumnya. Kelemahan utama yang terlihat di sini adalah bahwa sebagian besar organisasi hanya melihat biaya di muka solusi, bukan memfaktorkan biaya total kepemilikan (misalnya, pemeliharaan, dukungan, pelatihan, dan biaya tidak terduga lainnya). Bila item tersebut difaktorkan dalam perbandingan biaya, secara jelas keuntungan berada pada solusi berbasis SaaS.

**Gambar 11**
Perbandingan biaya antara solusi internal biasa dan SaaS.
Sumber: Penelitian Google

| Komponen Biaya | Vendor Perangkat atau Perangkat Lunak | Vendor SaaS |
|---|---|---|
| Perangkat Keras | | |
| Peningkatan perangkat email dan/atau server dibandingkan perkembangan organisasi dan spam | $2.000–$15.000 | t/a |
| Peningkatan perangkat email dan/atau server untuk pemulihan masalah | $2.000–$15.000 | t/a |
| Biaya tetap keseluruhan | $4.000–$30.000 | t/a |
| Perangkat lunak | | |
| Biaya lisensi | $1.000–$5.000 | $3.000–$12.000 |
| Biaya dukungan | $1.000–$5.000 | $0–$1.000 |
| Pemeliharaan | | |
| Penginstalan dan peningkatan kemampuan | $3.000–$5.000 | t/a |
| Administrasi dan konfigurasi | $4.000–$8.000 | $1.000–$2.000 |
| Dukungan pengguna akhir | $3.000–$6.000 | $1.000–$2.000 |
| Pelatihan | $2.000–$5.000 | minimal |
| Upaya pengalihan dan pemulihan | $2.000–$5.000 | tercakup |
| Biaya variabel keseluruhan (tahunan) | $16.000–$39.000 | $5.000–$17.000 |
| Biaya keseluruhan | $20.000–$69.000 | $5.000–$17.000 |

### Kesimpulan

Manfaat utama pendekatan SaaS, yakni kemudahan penerapan dan penggunaan, fleksibilitas administrasi dan manajemen, efektivitas, biaya total kepemilikan yang rendah, serta skalabilitas dan keandalan, membuatnya tepat terutama untuk organisasi yang ingin mengurangi masalah produktivitas TI pada keamanan dan kepatuhan komunikasi seperti dijelaskan di atas. Karenanya, Google berharap dapat melihat peningkatan jumlah organisasi yang menggunakan dan menerapkan solusi keamanan dan kepatuhan komunikasi berdasarkan model SaaS pada tahun mendatang. Semakin banyak perusahaan yang memperoleh manfaat SaaS secara langsung, akan semakin nyaman mereka mempercayai vendor SaaS serta menyerahkan kontrol keamanan dan kepatuhan komunikasinya kepada penyedia SaaS.

## Prioritas Komunikasi Bisnis tahun 2008

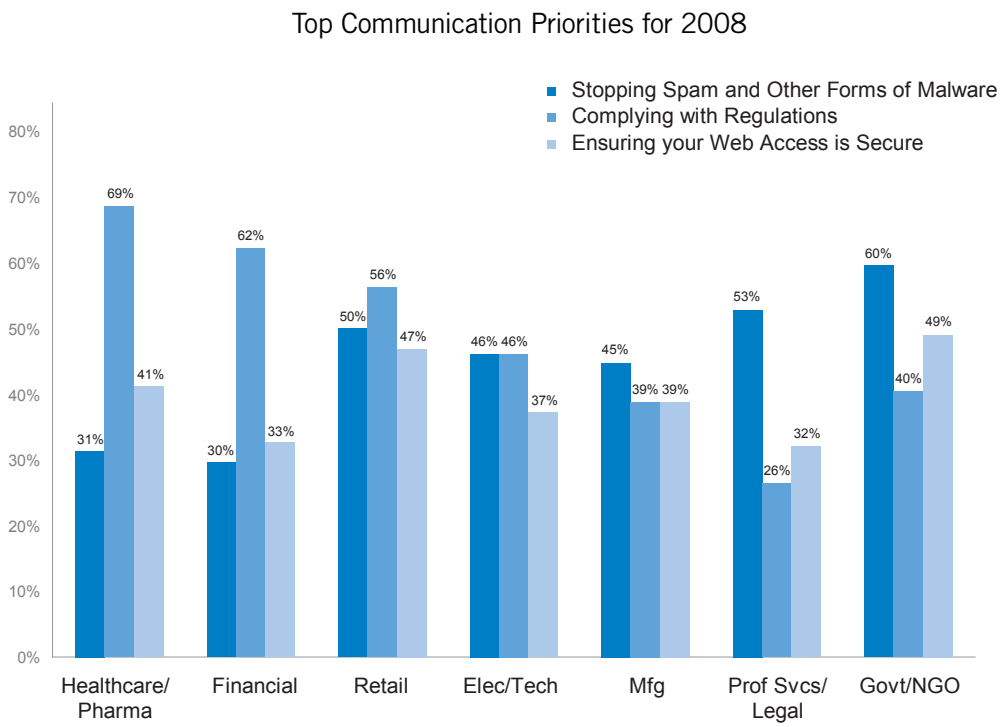
Sebagai bagian dari survei, Google juga meminta responden melihat masa depan serta memberitahukan prioritas keamanan dan kepatuhan komunikasi mereka untuk tahun mendatang. Sebagaimana diperkirakan, sebagian besar responden mencatat prioritas yang merupakan dampak langsung dari tren industri yang terjadi pada tahun 2007, seperti dijelaskan di bagian atas.

Yang patut dicatat adalah perbedaan prioritas di antara organisasi dalam berbagai segmen industri vertikal, misalnya keuangan, layanan kesehatan, ritel, dan pemerintahan. Kami memutuskan untuk menyorot perbedaan industri tersebut di bagian ini karena persoalannya begitu menyolok.

## Tiga prioritas teratas komunikasi bisnis

Meskipun menghentikan spam dan malware lainnya jelas merupakan prioritas utama dalam pemerintahan, namun layanan profesional/industri hukum, keuangan, dan layanan kesehatan lebih mengutamakan kepastian kepatuhan komunikasi bisnis terhadap peraturan pemerintah. Perbedaan ini tidak mengherankan karena keuangan dan layanan kesehatan adalah industri yang paling terpengaruh oleh peraturan, termasuk FINRA (Financial Industry Regulatory Authority) untuk keuangan dan HIPAA (Health Insurance Portability and Accountability Act) untuk layanan kesehatan. Karena harus memenuhi persyaratan kepatuhan yang nyata, industri ini cenderung menjadi tolok ukur pengaruh peraturan terhadap industri lainnya. Tentunya, semua perusahaan publik harus mematuhi persyaratan transparansi dan penyimpanan catatan SOX (Sarbanes Oxley Act).

**Gambar 12**
Identifikasi responden terhadap prioritas komunikasi utama untuk tahun 2008, dikelompokkan menurut industri.
Sumber: Penelitian Google

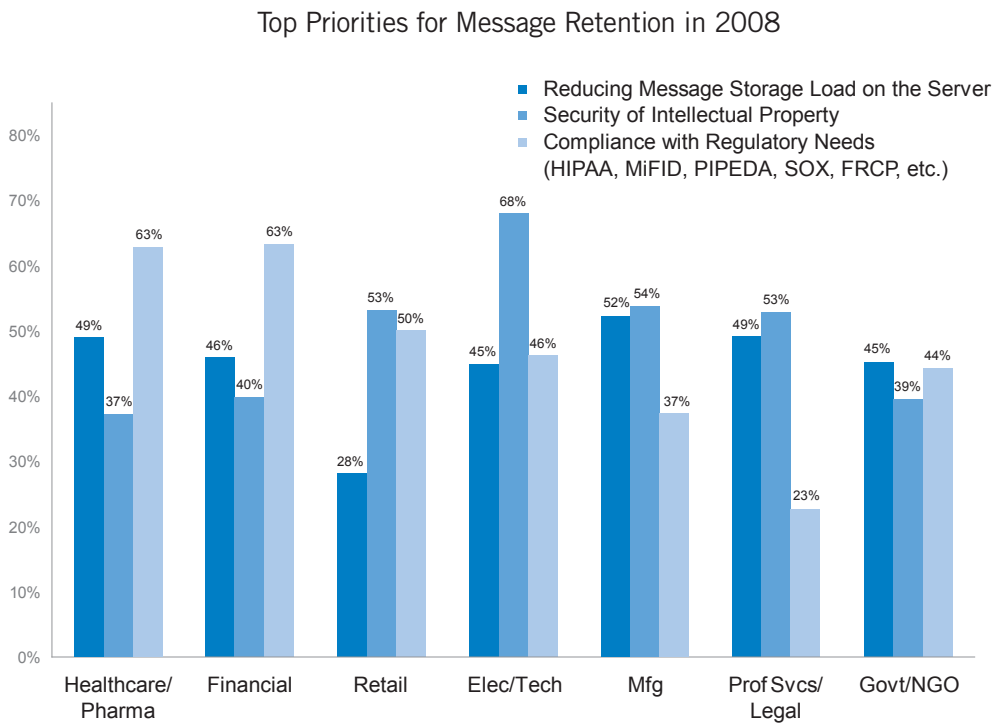



Satu hal yang menarik untuk dicatat adalah kenyataan bahwa akses Web yang aman untuk pertama kalinya menjadi salah satu dari tiga prioritas teratas bagi profesional komunikasi bisnis. Kemungkinan besar hal ini merupakan akibat adanya peningkatan dalam penggunaan interaksi pelanggan berbasis Web serta peningkatan serangan malware pada saluran komunikasi Web.

## Tiga prioritas teratas kepatuhan

Pada sisi kepatuhan, sekali lagi, terdapat perbedaan menonjol di antara industri. Dalam layanan keuangan dan layanan kesehatan, memastikan tersimpannya pesan untuk mematuhi petunjuk peraturan pemerintah adalah prioritas yang paling mendesak untuk tahun mendatang. Namun, bagi perusahaan teknologi, keamanan kekayaan intelektual untuk melindungi manfaat bersaing adalah prioritas utama, dengan hampir 70% perusahaan teknologi menjadikannya fokus utama untuk tahun 2008.

**Gambar 13**
Identifikasi responden terhadap prioritas retensi pesan untuk tahun 2008, dikelompokkan menurut industri.
Sumber: Penelitian Google




# Harapan Google untuk tahun 2008

Meskipun volume ancaman terhadap keamanan dan kepatuhan sistem pesan bisnis pada tahun 2008 tidak memiliki tingkat pertumbuhan yang sama seperti pada tahun 2007, kami mengantisipasi peningkatan kerumitan ancaman ini. Perusahaan akan menghadapi tantangan untuk mengidentifikasi berbagai jenis konten berbahaya baru serta melindungi informasi yang sensitif dari teknik rekayasa sosial. Tehnik tersebut berupaya menghindari tindakan keamanan dengan memanipulasi atau menipu pengguna untuk mengungkapkan atau melakukan tindakan yang mengungkapkan data rahasia. Untuk menghindari kemungkinan kebocoran data, kami mengharapkan setiap organisasi untuk meningkatkan penekanan terhadap kebijakan keamanan keluar serta enskripsi konten pada tahun mendatang.

Berikut adalah beberapa tantangan lainnya yang akan dihadapi perusahaan pada tahun 2008:

- Volume spam akan stabil dan bahkan menurun pada tahun 2008 karena serangan spam akan lebih terarah. Namun, karena semakin banyaknya konten spam yang terdapat dalam lampiran email, kami memperkirakan volume spam akan kerap berubah.
- Serangan virus akan terus bercampur dengan spam disertai peningkatan fokus pada pencurian identitas menggunakan teknik rekayasa sosial canggih yang terkait dengan acara khusus, seperti Super Bowl, Olimpiade Musim Panas, bencana alam, dan sebagainya. Serangan virus juga akan mengincar eksekutif pada perusahaan tertentu dengan kekayaan intelektual yang dianggap berharga di pasar gelap oleh hacker. Serangan ini akan tampak berasal dari agensi bisnis yang sah, seperti Internal Revenue Service, Better Business Bureau, serta Securities and Exchange Commission. Google memperkirakan akan lebih banyak muncul jenis serangan ini sepanjang tahun yang akan mengakibatkan pelanggaran data penting pada perusahan komersil dan lembaga pemerintah. Kami juga mengantisipasi modifikasi penerapan email yang terpaksa dilakukan oleh perusahaan akibat pelanggaran data, seperti menghapus link pintas dalam komunikasi email pelanggan.

- Akan semakin banyak perusahaan dan organisasi yang menerapkan kebijakan khusus yang mengatur konten keluar dalam email dan menggunakan sistem agar dapat memantau dan menjalankan kebijakan tersebut untuk mencegah kebocoran data rahasia atau sensitif.
- Meningkatnya kebutuhan untuk mengelola privasi data konsumen dan kebijakan penyimpanan secara global akan mendorong peningkatan enkripsi dan pengarsipan. Selain itu, beberapa solusi yang di-host (SaaS) akan berperan penting dalam mengurangi biaya dan kerumitan produk ini.
- Akan semakin banyak serangan pencurian identitas yang diluncurkan dari situs Web, terutama situs yang memungkinkan pengguna membuat konten sendiri, misalnya situs jaringan sosial, blog, dan situs pelelangan.
- Seiring semakin banyaknya negara bagian yang merevisi peraturan tentang prosedur sipil untuk pengadilan negeri (mirip dengan F ederal Rules of Civil Procedure), organisasi harus membuat rencana kesiapan litigasi yang mendorong pengarsipan pesan elektronik dan solusi e-discovery.

## Penerapan Tbaik Komunikasi Bisnis tahun 2008

Bagaimana cara Anda mempersiapkan perusahaan untuk menghadapi tantangan keamanan pesan dan kepatuhan yang dijelaskan dalam laporan ini? Berdasarkan pengalaman dan penelitian Google, berikut adalah beberapa penerapan terbaik untuk mengatasi masalah pada tahun depan:

### Penerapan terbaik keamanan

1. **Melindungi organisasi Anda.** Gunakan solusi antispam dan antimalware di seluruh perusahaan Anda dan selalu perbarui solusi tersebut. Bila memungkinkan, tingkatkan solusi SaaS agar dapat melepaskan beban untuk selalu memperbarui pertahanan. Pada banyak kasus, Anda dapat menurunkan biaya dan mengurangi dampak terhadap sumber daya IT dengan menggunakan solusi SaaS.
2. **Mengikuti perkembangan terkini.** Ikuti perkembangan semua aplikasi terkini hingga ke tingkat patch terbaru. Hal ini terutama berlaku untuk sistem operasi, browser Web, pembaca file (misalnya, Adobe Acrobat Reader), pemutar multimedia, dan aplikasi lain yang biasanya diluncurkan dari browser Web.
3. **Memberikan informasi pengguna sesering mungkin.** Terus ingatkan dan berikan informasi kepada pengguna tentang ancaman eksternal dan kebijakan perusahaan internal perihal penggunaan email. Jika terjadi gangguan terhadap pertahanan, cari cara untuk segera mengkomunikasikannya kepada pengguna agar mereka mewaspadai ancaman tersebut.
4. **Menetapkan kebijakan penggunaan email dengan mengutamakan keamanan.** Misalnya, tentukan cara menangani lampiran tertentu seperti eksekusi, script, file multimedia, dsb. Identifikasikan kebijakan global dan pengecualian kelompok. Komunikasikan kebijakan tersebut secara teratur kepada karyawan Anda dan gunakan sistem fleksibel yang tidak hanya dapat memantau dan menjalankan kebijakan ini, namun juga dapat berubah seiring perkembangan kebijakan.
5. **Mengidentifikasi konten sensitif.** Identifikasikan konten yang terdapat dalam pesan email masuk dan keluar yang mungkin sensitif, rahasia, atau pribadi. Buat kebijakan email yang menangani jenis data ini dan gunakan solusi yang

memungkinkan Anda memantau dan menjalankan kebijakan konten. Misalnya, sistem yang secara otomatis dapat mengenkripsi email sensitif dapat bermanfaat bagi perusahaan yang mungkin diwajibkan untuk memahami pribadi. Sistem ini harus fleksibel secara khusus dalam bereaksi terhadap konten yang terus berubah dan terdapat dalam email.

6. **Mengevaluasi penggunaan Web perusahaan.** Tetapkan kebijakan tentang penggunaan Web yang dapat diterima di organisasi Anda. Pertimbangkan penggunaan solusi yang dapat memantau akses Web dan memberikan perlindungan antimalware secara real-time yang mirip dengan keamanan email yang telah digunakan. Ancaman malware di Web lebih cepat berkembang secara nyata dibandingkan ancaman berbasis email dan banyak perusahaan memiliki perlindungan terbatas atau saat ini tidak memilikinya.

### Penerapan terbaik kepatuhan

1. **Merencanakan ke depan.** Jangan tunggu hingga muncul gugatan hukum, keluhan lingkungan kerja yang tidak ramah, terjadinya kebocoran rahasia dagang, atau hilangnya informasi rahasia untuk mulai mengelola data Anda.
2. **Mengetahui apa yang diharuskan oleh hukum.** Pahami persyaratan hukum industri serta wilayah hukum lokasi perusahaan beroperasi. Misalnya, apakah kewajiban penyimpanan data untuk informasi tertentu di sebuah negara atau negara bagian? Jika ada, perlindungan apakah yang ada untuk membatasi akses atau penyimpanan? Apakah Anda mengetahui data yang harus dienkripsi dan kewajiban pemberitahuan yang berlaku jika terjadi pelanggaran keamanan? Apakah penyaring dianggap penting di wilayah hukum untuk menghindari lingkungan kerja yang tidak ramah atau apakah penyaringan dianggap sebagai pelanggaran privasi?
3. **Satu solusi mungkin tidak mencakup semua hal.** Jika Anda beroperasi pada skala nasional atau internasional, pahami bahwa sistem manajemen data elektronik harus memenuhi kewajiban yang terkadang bertentangan. Coba firewall, pembatasan akses, dan penonaktifan fungsi tertentu dalam wilayah hukum, misalnya yang tidak mengizinkan pemantauan atau penyaringan.
4. **Melimpahkan tanggung jawab untuk mengelola sistem.** Tunjuk staf yang bertanggung jawab atas penyimpanan dan manajemen data elektronik. Anda dapat menugaskan beberapa orang dari divisi legal dan TI dengan saran dari SDM atau divisi lainnya. Sejak awal, libatkan semua orang yang akan memfungsikan sistem bila timbul kewajiban hukum.
5. **Mencari berbagai bentuk dan penyimpan data.** Ingat bahwa data dapat disimpan di meja kerja, PDA (personal digital assistant), komputer rumah, laptop, dan di tempat lainnya. Agar dapat mengelola data yang secara hukum menjadi akuntabilitas perusahaan, Anda harus terlebih dulu mengidentifikasi tindakan dan lokasi untuk memastikan sistem yang digunakan akan mengambil data relevan. Ketahui metadata yang Anda miliki.
6. **Jangan simpan yang tidak diperlukan.** Jangan menyimpan terlalu banyak data elektronik hanya karena teknologi membuat Anda mampu melakukannya. Penyimpanan data yang tidak diperlukan bukan hanya akan memperumit pengambilan data, namun juga dapat meningkatkan risiko hacking. Misalnya, jangan menyimpan data keuangan pelanggan yang sensitif kecuali jika dibutuhkan. Jika memerlukannya, enkripsikan.

**SELENGKAPNYA**

www.google.com/a/security

# Kesimpulan

Perkembangan yang berkelanjutan dalam sistem pesan elektronik diiringi peningkatan spam adalah duri dalam daging bagi profesional TI. Di sebagian besar organisasi, divisi TI bertanggung jawab memastikan keamanan dan kesesuaian komunikasi eletronik, namun rintangan menuju keberhasilan cukup besar.

Profesional TI saat ini tidak hanya menghadapi ancaman spam, virus, dan worm, namun mereka juga berupaya mengamankan staf lapangan yang semakin bertambah, memastikan ketersediaan dan kesinambungan proses bisnis penting, memenuhi tujuan kesesuaian, merencanakan pemulihan masalah, pencegahan kebocoran data, dan melindungi sistem internal dari hacker. Tidak heran jika profesional TI mengalami masalah terbesar pada tingkat produktivitas.

Solusi SaaS pada umumnya dan layanan keamanan dan kesesuaian pesan Google pada khususnya menangani masalah produktivitas TI ini dan membantu organisasi mengatasi ancaman dalam sistem pesan elektronik. Dengan menggunakan layanan Google, organisasi dapat mengurangi masalah dalam memastikan keamanan dan kesesuaian serta meningkatkan produktivitas profesional TI.

Google™