STUDI KELAYAKAN DISASTER RECOVERY PLAN PADA INFRASTRUKTUR JARINGAN KOMPUTER (STUDI KASUS JARINGAN KOMPUTER UNIVERSITAS WIDYATAMA)

Nilla Rachmaningrum[1)], Falahah[2)]
[1,2)] Program Studi Teknik Informatika
Fakultas Teknik, Universitas Widyatama
Jl. Cikutra 204A Bandung 40124
email : nilla.racmaningrum@widyatama.ac.id[1)], falahah@widyatama.ac.id[2)]

Abstrak

Disaster recovery plan (DRP) adalah rencana yang disiapkan organisasi untuk membantu organisasi pulih setelah terjadi musibah atau bencana. Penyebab musibah bervariasi, mulai dari fenomena alam hingga akibat perbuatan manusia, baik yang disengaja maupun tidak disengaja. Pada bidang teknologi informasi, penyebab dapat lebih spesifik misalnya kegagalan infrastruktur , kekeliruan operator, hingga serangan virus. Tingginya kebergantungan organisasi pada infrastruktur teknologi informasi menyebabkan perlunya dipertimbangkan DRP di bidang infrastruktur jaringan komputer.

DRP perlu dibuat dengan tepat dan optimal, sesuai dengan kebutuhan dan kemampuan organisasi. Untuk itu, diperlukan studi awal untuk melihat kelayakan organisasi atas kebutuhan adanya DRP. Pada penelitian ini dilakukan studi kelayakan diperlukannya DRP pada infrastruktur jaringan komputer, dengan studi kasus pada jaringan komputer Universitas Widyatama. Studi kasus dilakukan dengan menginventarisir kondisi infrastruktur jaringan serta mengamati tingkat kebergantungan sivitas akademika dan proses bisnis di Universitas Widyatama terhadap infrastruktur jaringan komputer. Hasil studi menujukan bahwa rendahnya tingkat kesadaran pengamanan data terhadap bencana, dari sebagian besar pengguna, yang diikuti oleh tingginya tingkat kebergantungan terhadap ketersediaan layanan jaringan komputer. Inventarisir kondisi infrastruktur jaringan juga menunjukan belum adanya tendensi dan kesiapan dalam menghadapi bencana. Hasil akhir penelitian merekomendasikan perlunya disiapkan sebuah DRP untuk infrastruktur jaringan komputer untuk membantu pihak manajemen menyelamatkan informasi penting di saat terjadi bencana.

Kata kunci : *disaster recovery, jaringan komputer, kelayakan, studi kasus.*

1. PENDAHULUAN

Seperti umum diketahui, teknologi informasi merupakan salah satu kebutuhan mendasar hampir di semua sector bisnis, seperti halnya kebutuhan akan listrik dan telpon. Teknologi informasi, dalam konteks teknis, dapat diartikan sebagai sekumpulan infrastruktur untuk mendukung pengelolaan informasi yang meliputi proses *collect, store, retrieve, disseminate* dan *reusable* of information. Disadari atau tidak, dewasa ini, hampir semua sektor bisnis mempercayakan informasi penting perusahaannya pada sederetan peralatan teknologi informasi atau lazim kita sebut dengan infrastruktur. Tetapi, tingginya tingkat kebergantungan ini jarang sekali disertai dengan kesadaran akan adanya ancaman kerusakan infrastruktur, yang umumnya terjadi secara tidak terduga, baik akibat pengaruh dari lingkungan internal maupun eksternal, baik yang disengaja maupun tidak.

Dinamisnya lingkungan bisnis saat ini dan juga perubahan situasi lingkungan alam, sosial dan politik, menimbulkan adanya ancaman baru yang mungkin sebelumnya tidak terlalu dipikirkan dengan sungguh-sungguh. Adanya ancaman dari lingkungan alam seperti bencana alam, ataupun lingkungan sosial politik seperti kerusuhan, atau musibah lainnya seperti kebakaran, kerusakan layanan listrik dan lain-lain telah menempatkan informasi yang selama ini dititipkan pada infrastruktur teknologi informasi dalam posisi yang rawan. Paradigma baru seperti *paperless office* atau *office automation* yang menempatkan informasi dalam bentuk digital sebagai pengganti informasi fisik berupa kertas atau dokumen juga turut menambah tingginya resiko kehilangan informasi akibat kasus bencana.

Dalam konteks ini, ada baiknya perusahaan atau organisasi mulai memikirkan antisipasi yang sungguh-sungguh untuk menyelamatkan informasi yang sangat berguna bagi kelangsungan bisnis, terutama setelah bencana terjadi. *Business continuity* atau keberlangsungan bisnis setelah satu bencana juga turut dijadikan salah satu parameter penilaian kematangan manajemen dalam mengelola sumber daya yang dimiliki di satu organisasi. Salah satu elemen penting pada *business continuity* yaitu *disaster recovery plan(DRP*), atau penyusunan rencana pemulihan setelah terjadinya bencana.

Wujud DRP sendiri secara sederhana hanya berupa dokumen yang berisi *response plan* (rencana tanggap) terhadap bencana. Tetapi, proses penyusunan dokumen tersebut tidaklah mudah dan memerlukan pengetahuan yang mendalam mengenai berbagai resiko yang dihadapi perusahaan / organisasi. Ruang lingkup DRP dapat dibuat melebar meliputi infrastruktur, personel dan prosedur [1]. Pada tulisan ini, fokus pembahasan DRP ditekankan pada DRP terkait dengan penyelamatan infrastruktur teknologi informasi dari ancaman bencana.

Indonesia sendiri, dalam 10 tahun terakhir sudah mengalami beberapa kali bencana besar yang tidak pernah diduga sebelumnya, seperti tsunami di Aceh (2004), gempa di Yogyakarta (2006), letusan gunung berapi dan beberapa kejadian serupa dalam skala yang lebih kecil. Catatan kerugian yang ada saat ini berfokus pada kehilangan nyawa manusia dan kerugian materil berupa kerusakan infrastruktur jalan dan bangunan. Hingga saat ini belum ada data atau penelitian yang dapat memberikan gambaran besarnya kerugian akibat rusak/hilangnya informasi atau rusak/hilangnya infrastruktur teknologi informasi. Untuk itu, ada baiknya organisasi-organisasi di Indonesia mulai meluangkan waktu dan pikiran untuk menyusun semacam DRP bagi organisasinya sendiri.

Universitas, sebagai salah satu organisasi yang mengemban amanah masyarakat untuk menyelenggarakan pendidikan, tidak terlepas dari kewajiban memelihara informasi dan menjaga eksistensi informasi tersebut terhadap berbagai ancaman musibah ataupun kecelakaan lainnya. Beberapa universitas terkemuka di benua Amerika dan Eropa sudah melengkapi diri dengan DRP yang disajikan dalam bentuk dokumen resmi. Atas dasar fakta tersebut maka pada penelitian ini akan dicoba dilakukan kajian awal kesiapan terhadap bencana, khususnya yang terkait pada usaha penyelamatan infrastruktur layanan jaringan komputer, dengan studi kasus di Universitas Widyatama.

2. DISASTER RECOVERY PLAN (DRP)

DRP adalah proses, kebijakan dan prosedur yang berkaitan dengan persiapan pemulihan atau keberlangsungan infrastruktur teknologi yang kritis bagi organisasi setelah terjadinya bencana, baik bencan yang disebabkan oleh tindakan manusia ataupun bencana alam. *Disaster recovery* merupakan bagian dari *business continuity*. Sedangkan *business continuity* sendiri merupakan aktivitas yang dilakukan oleh organisasi untuk menjamin bahwa fungsi bisnis kritis dapat tetap tersedia bagi konsumen, supplier dan pihak-pihak lainnya yang berkepentingan [3].

Perencanaan *disaster recovery* mengacu pada persiapan untuk menghadapi bencana dan respon yang harus diberikan ketika bencana terjadi. tujuan DRP adalah keberlangsungan (*continuity*) atau kemampuan organisasi untuk bertahan (survival) dalam menghadapi bencana (Proses penyusunan DRP meliputi analisis, perencanaan, pembuatan DRP, pengujian dan revisi periodik berdasarkan kondisi bisnis terkini[2].

Beberapa jenis bencana yang dapat mengancam bisnis dapat dikelompokkan berdasarkan penyebab sebagai berikut : bencana alam, bencana akibat kegagalan alat-alat, akibat kegagalan aspek keamanan, dan situasi lingkungan seperti demonstrasi, terorisme, perang, sabotase dan lain-lain.

Berbagai macam penyebab kejadian bencana di atas, dapat berpotensi menyebabkan kerusakan pada gedung, peralatan dan sistem teknologi informasi. Dampak bencana terhadap organisasi dapat berupa *direct damage* (kerusakan langsung alat-alat dan gedung), *inaccessibility* (fasilitas tidak dapat diakses), *utility outage* (tidak tersedianya infrastruktur pendukung seperti listrik,air dan sebagainya), *transportation disruption, communication disruption, evacuation* dan *worker absenteeism* [2]. Dampak tersebut dapat menghentikan bisnis baik untuk sementara atau hingga jangka waktu tertentu. Jika terhentinya bisnis ini terus berlanjut,dapat mengakibatkan pindahnya para konsumen ke pelaku bisnis lainnya.

Bencana yang diuraikan di atas adalah bencana skala besar yang seringkali dianggap "jarang" terjadi. Bencana dalam skala kecil biasanya lebih sering terjadi misalnya kebakaran, kebocoran pipa saluran air, atau jenis kerusakan lainnya yang berasal dari kerusakan di luar lingkungan komputer. Lebih sering lagi adalah bencana yang diakibatkan oleh perbuatan manusia yang sengaja atau tidak sengaja seperti kegagalan aplikasi, kegagalan hardware, hacking, serangan virus, Denial of services dan sabotase internal lainnya.

Tingkat dan dampak kerusakan infrastruktur, khususnya infrastruktur teknologi informasi, bagi suatu organisasi sangat beragam, tergantung sejauh mana kebergantungan organisasi tersebut terhadap teknologi informasi. Salah satu cara untuk meminimalisasi dampak kerusakan tersebut adalah menyiapkan DRP yang paling optimal untuk suatu organisasi. DRP yang pada dekade tahun 90-an tidak terlalu menjadi perhatian di kalangan bisnis, sejak tahun 2000-an mulai banyak diperhatikan oleh berbagai pihak. DRP yang pada awalnya hanya diprioritaskan untuk menyelamatkan nyawa manusia, dikembangkan juga kea rah penyelamatan infrastruktur. Seiring dengan meningkatnya kebergantungan bisnis terhadap teknologi informasi maka meningkat juga resiko ancaman akibat bencana terhadap keberlangsungan bisnis. Saat ini bahkan sudah diterbitkan pedoman standar khusus sebagai pedoman penyusunan dan evaluasi DRP, khusus untuk operasional dan manajemen teknologi informasi, yaitu ISO/IEC 24762:2008 yang menyediakan pedoman penyusunan DRP untuk teknologi informasi dan komunikasi. Pedoman ini merupakan bagian dari dari manajemen business continuity, dan diterapkan baik bagi penyedia layanan

teknologi informasi dan komunikasi internal (*information communication technology-ICT*) maupun eksternal (*outsourced*), dan meliputi fasilitas fisik dan layanan. Spesifikasi ISO/IEC 24762:2008 meliputi [4]:

1. Kebutuhan untuk menerapkan, mengoperasikan, memonitor dan memelihara fasilitas dan layanan disaster recovery untuk ICT.
2. Kemampuan yang harus dimiliki oleh layanan disaster recovery ICT eksternal dan pedoman praktis yang harus dijalankan untuk menyediakan lingkungan operasional minimal yang aman dan memfasilitasi usaha organisasi untuk melakukan recovery.
3. Pedoman memilih situs recovery dan pedoman untuk peningkatan layanan disaster recovery ICT

Penyusunan DRP untuk teknologi informasi di suatu organisasi, secara umum mengacu pada langkah-langkah pengelolaan proyek pada umumnya, yaitu : inisialisasi, eksekusi dan evaluasi. Pada tahap inisialisasi, diperlukan dukungan manajemen dan kontrak proyek yang jelas antara manajemen yang berwenang dengan pihak yang akan menyusun DRP. Kontrak proyek ini diperlukan untuk menjaga konsistensi komitmen semua pihak yang terlibat. Pada tahap eksekusi, dilakukan sekumpulan aktivitas yang keluaran akhirnya diharapkan dapat menghasilkan dokumen DRP yang sesuai dengan kondisi dan kebutuhan organisasi. Aktivitas tersebut antara lain [2]:

1. Melakukan *business impact analysis*, yang meliputi penentuan *maximum tolerable downtime* (MTD), penentuan *recovery objective* yang meliputi *recovery time objective* (RTO), dan *recovery point objective (RPO)*, membuat analisis resiko, menyajikan semua hasil analisis dalam satu laporan terintegrasi.
2. Mendefinisikan *prosedur recovery*, yaitu membuat DRP untuk setiap proses dengan cara memetakan proses dengan infrastruktur, membuat DRP dalam bentuk tertulis, dan menguji DRP tersebut.
3. Evaluasi dan monitoring meliputi proses pengujian dan kaji ulang secara periodik misalnya setiap bulan, setiap 4 bulan atau tahunan. Tahap lainnya yaitu memberikan pelatihan yang memadai bagi semua tim DRP yang terlibat, khususnya tim *recovery*.

Sebuah dokumen DRP idealnya memuat elemen-elemen berikut [1]:

1. Prosedur deklarasi keadaan dalam bencana
2. Nama dan alamat yang dapat dihubungi dalam keadaan darurat
3. Tim tanggap darurat
4. Prosedur penilaian tingkat kerusakan
5. Prosedur *recovery* dan *restart* sistem
6. Transisi ke kondisi normal
7. Tim *recovery*

Meskipun DRP merupakan satu elemen penting bagi keberlangsungan bisnis, tetapi masih banyak organisasi yang mengabaikannya dan membiarkan seluruh kepentingan bisnis organisasi pada kondisi yang "pasrah" terhadap peluang ancaman musibah. Kondisi kontradiktif tersebut disebabkan oleh berbagai factor yang memicu pro dan kontra misalnya [1] :

1. Besarnya biaya yang harus disiapkan untuk mendukung DRP, baik prosedur maupun infrastruktur. Biasanya biaya untuk penyiapan infrastruktur cadangan sangat besar, dan tidak ada kepastian apakah infrastruktur cadangan tersebut akan benar-benar terpakai.
2. Tidak jelasnya target recovery yang ingin dicapai. Mencapai recovery maksimal mungkin merupakan kondisi ideal, tetapi kondisi ini tidak dapat dicapai tanpa pengorbanan yang besar dan tidak ada jaminan bahwa pengorbanan yang besar tersebut pasti akan mencapai tingkat target recovery maksimal.
3. Optimalisasi infrastruktur masih diprioritaskan pada dukungan operasional organisasi, tidak untuk alokasi sesuatu yang tidak pasti terjadi.

Salah satu alternatif untuk mengurangi kontradiksi di atas serta memberikan bahan pertimbangan yang obyektif kepada manajemen yaitu dengan melakukan suatu studi kelayakan sebelum mengusulkan sebuah DRP. Studi kelayakan ini ditujukan untuk mengungkap kelemahan dan kekuatan organisasi secara rasional dan obyektif untuk mengahadapi peluang dan tantangan yang berada di lingkungan organisasi tersebut (Wikipedia). Termasuk pada kriteria kelayakan yaitu biaya dan nilai yang diperoleh

3. STUDI KELAYAKAN DRP PADA INFRASTRUKTUR JARINGAN KOMPUTER

Pada penelitian ini, akan dilakukan sebuah studi kelayakan awal pada infrastruktur jaringan komputer di suatu organisasi dengan tujuan untuk melihat sejauh mana organisasi tersebut memerlukan DRP. Penelitian ini dilakukan di Universitas Widyatama Bandung dan dibatasi pada infrastruktur jaringan komputer yang dikelola di bawah Pusat Teknologi Informasi Universitas.

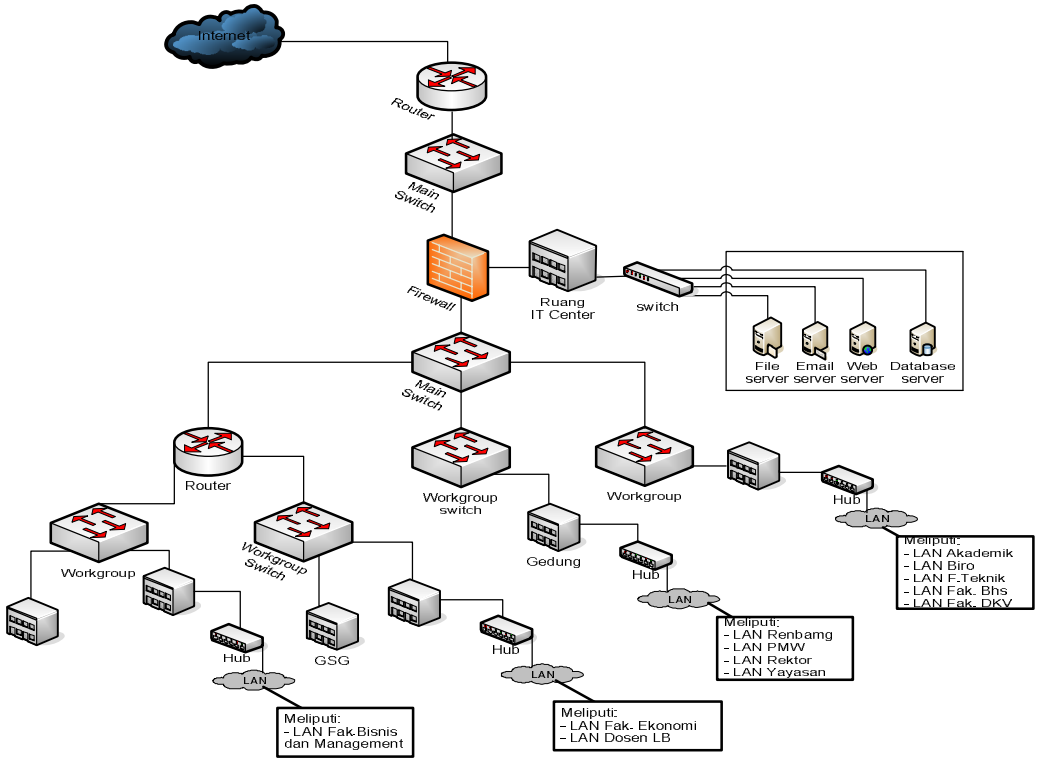
Metoda yang digunakan pada penelitian ini meliputi studi literatur tentang aspek-aspek DRP, observasi lapangan dan pemberian rekomendasi atas temuan-temuan yang dihasilkan. Observasi lapangan meliputi inventarisasi infrastruktur dan penyebaran kuisioner untuk melihat tingkat kebergantungan sivitas akademika dan proses bisnis di Universitas Widyatama terhadap infrastruktur jaringan.

Universitas Widyatama yang berdiri mulai 2 Agustus 2001, merupakan gabungan dari berbagai perguruan tinggi yang sudah ada sebelumnya yaitu STIEB, STIBB, STDKV, STTB dan Magister Manajemen. Saat ini Universitas Widyatama sudah menerapkan sistem pelayanan pendidikan dengan standar ISO-9001:2008 untuk sekitar 7000 mahasiswanya yang tersebar di 5 fakultas yaitu Fakultas Bisnis dan Manajemen, Teknik, Ekonomi, Bahasa dan Desain Komunikasi Visual.

Dalam pelaksanan Tridarma Perguruan Tinggi, Universitas Widyatama mengimplementasikan berbagai sistem informasi dan aplikasi pada jaringan komputer yang sudah ada, misalnya sistem informasi akademik, sistem *e-campus* yang berperan sebagai portal komunikasi mahasiswa dengan informasi di kampus, *e-LMS*, *e-Library*, dan beberapa aplikasi lainnya yang dapat diakses dari dalam dan luar kampus. Pengelolaan dan pemeliharaan jaringan komputer di Universitas Widyatama dikelola secara terpusat oleh Pusat Teknologi Informasi, dengan topologi jaringan seperti pada gambar 1.

Adanya beberapa aplikasi yang diakses dari luar kampus dan penggunaan jasa *cloud service* seperti *Google Application* membuat pihak pengelola PTI kampus menerapkan *DMZ* sebagai strategi pengamanan jaringan internal. DMZ (*Demilitarized Zone*) – atau jaringan perimeter adalah jaringan *security boundary* yang terletak diantara suatu jaringan *corporate / private* LAN dan jaringan publik (Internet). *Firewall* DMZ ini dibuat untuk pengamanan jaringan yang mengijinkan *server* internal dapat diakses oleh publik dengan aman tanpa harus mengganggu keamanan sistem jaringan internal. Perimeter (DMZ) *network* dirancang untuk melindungi *server* pada jaringan LAN *corporate* dari serangan *hackers* dari Internet [5].

Saat ini, semua *server* yang memuat semua aplikasi internal disimpan dalam satu ruangan dan tidak ada pembagian khusus untuk *server-server* tersebut. Mekanisme pemeliharaan jaringan dibagi menjadi dua lapisan yaitu lapisan *intermediate* yang meliputi perawatan peralatan jaringan seperti *router, switch* dan lain-lain, dan lapisan *end-user* yang meliputi perawatan kabel, konektor hingga komputer yang digunakan oleh *end-user*. Antivirus dipasang baik pada *server* maupun di komputer yang digunakan klien. Mekanisme antisipasi *recovery* tidak disiapkan dengan baik, ditandai dengan tidak adanya mekanisme yang jelas untuk proses *backup* dan *recovery* antar *hard disk* pada *server* ataupun antar *server*.



Gambar 1. Topologi Infrastruktur Jaringan Komputer Universitas Widyatama

Pada penelitian ini juga dilakukan semacam survey awal untuk melihat perilaku pengguna jaringan komputer di Universitas Widyatama, untuk menilai tingkat kebergantungan pengguna dan pelaksanaan proses bisnis terhadap infrastruktur jaringan komputer. Survey disebarkan kepada sekitar 60 responden, meliputi 30 mahasiswa, 15 dosen dan 15 pegawai. Jumlah *sample* responden yang kecil dipilih karena penelitian ini baru bersifat studi awal yang akan digunakan untuk pengembangan penelitian yang lebih spesifik lagi. Responden dari pihak dosen dan pegawai dipilih berdasarkan tingkat kebergantungan terhadap infrastruktur jaringan komputer. Hal ini karena tidak semua dosen dan pegawai aktif menggunakan fasilitas jaringan komputer universitas, sehingga tidak dapat mewakili ekspektasi terhadap ketersediaan layanan jaringan komputer. Tabel 1 menunjukan hasil survey terhadap beberapa parameter untuk melihat tingkat kebergantungan pengguna berdasarkan perilaku pengguna. Tabel 2 menunjukan jenis proses bisnis yang saat ini didukung oleh infrastruktur jaringan komputer universitas.

Tabel 1. Parameter Kebergantungan Pengguna terhadap Infrastruktur Jaringan Komputer

Parameter	**Mahasiswa**	**Dosen**	**Pegawai**
Lama akses ke jaringan	2-3 jam /hari	2-3 jam/hari	3-4 jam/hari
Cara akses	*WIFI, wired*	*Wired*	*wired*
Media komunikasi internal	*Email, chatting*, forum, *social networking*	*Email, chatting*, forum	*Email, chatting*
Jenis aplikasi yang diakses	*Email, e-campus, e-library, e-LMS*	*Email, e-library, e-LMS*	*Email*, aplikasi pendukung pekerjaan.
Pemahaman tentang keamanan jaringan	Kurang	Kurang	Sangat kurang
Tindakan pengamanan terhadap data	Jarang	Jarang	Sangat jarang

milik sendiri			
Parameter	**Mahasiswa**	**Dosen**	**Pegawai**
Bentuk pengamanan yang digunakan	*Password*, enkripsi, *backup*	*Password*, enkripsi, *backup*	*Password*, enkripsi
Penitipan *file* di *server* Universitas	Tidak ada	Tidak ada	Sesuai aplikasi yang digunakan
Ekspektasi terhadap ketersediaan layanan jaringan komputer	Sedang	Tinggi	Sangat tinggi
Tingkat kebergantungan terhadap ketersediaan layanan jaringan komputer	Sedang	Tinggi	Sangat tinggi

Hasil rekapitulasi data pada Tabel 1 dibuat dalam bentuk deskriptif dan tidak dalam bentuk angka, dipilih berdasarkan jawaban yang paling dominan untuk setiap parameter pengamatan. Hasil ini menunjukan kondisi yang agak kontradiktif antara tingginya tingkat kebergantungan terhadap infrastruktur jaringan tetapi rendahnya tindakan pengamanan terhadap data milik sendiri. Secara implisit hal ini menyatakan bahwa sebagian pengguna jaringan komputer mengandalkan dan mempercayakan data mereka pada jaringan komputer universitas. Bentuk pengamanan berupa *backup* juga dilakukan oleh pengguna tidak dalam perioda tertentu, tetapi sesuai dengan kebutuhan dan disimpan dalam bentuk salinan *file* pada *storage* external seperti *flashdisk* atau *external hard-disk* milik pribadi. Tingginya tingkat kebergantungan pegawai pada layanan jaringan komputer karena hampir semua pekerjaan mereka mengharuskan pengolahan dan pertukaran data melalui komputer. Tetapi, tidak adanya penitipan *file* yang teroganisir di *server* milik universitas, kecuali yang berbasis aplikasi, menyebabkan *file-file* penting tersebar di setiap komputer yang digunakan oleh dosen/pegawai.

Tabel 2 menunjukan beberapa aplikasi yang berjalan di atas infrastruktur jaringan komputer. Aplikasi-aplikasi ini sangat penting untuk mendukung kegiatan belajar-mengajar dan administrasi operasional sehari-hari. Tidak adanya informasi mengenai aktivitas *backup* untuk setiap aplikasi menunjukan kurangnya kepedulian pemilik data dan manajemen dalam antisipasi menghadapi bencana.

Tabel 2. Penggunaan Infrastruktur Jaringan Komputer untuk Mendukung Proses Bisnis

Proses Bisnis	**Penggunaan infrastruktur jaringan**
Perwalian	
Penjadwalan kuliah	
Pengumuman jadwal kuliah dan Ujian	✓
Pengumuman nilai	✓
Absensi dan penggajian karyawan	✓
Daftar Ulang	
Administrasi Keuangan	✓
Administrasi Kepegawaian	✓
Pengelolaan buku perpustakaan	✓
Pertukaran dokumen	✓

Berdasarkan temuan-temuan tersebut, penelitian ini merekomendasikan beberapa hal sebagai berikut :

1. Perlu dilakukan inisiatif penyusunan DRP untuk infrastruktur jaringan komputer mengingat banyaknya aktivitas yang bergantung pada layanan jaringan komputer dan rendahnya tingkat kesadaran pengguna terhadap pentingnya proses pengamanan data milik sendiri ataupun data-data terkait pekerjaan masing-masing.
2. Kelayakan diperlukannya DRP didukung oleh fakta bahwa secara teknis, saat ini implementasi jaringan komputer universitas juga belum mengadopsi kebutuhan ke arah tersebut. Hal ini dapat dilihat dari fakta bahwa semua server penting disimpan pada satu ruangan dan tidak ada mekanisme backup dan recovery pada setiap server tersebut.
3. Perlu studi lanjut untuk menetapkan tingkat DRP yang paling optimal yang disesuaikan dengan kemampuan dan kebutuhan, dengan memperhatikan biaya dan manfaat DRP tersebut bagi Universitas Widyatama.

4. KESIMPULAN

1. Disaster Recovery Plan di bidang teknologi informasi merupakan salah satu aspek penting dalam mendukung keberlangsungan bisnis setelah terjadinya bencana, untuk mempertahakan semua pihak yang terlibat pada bisnis tersebut termasuk konsumen dan pelaku bisnis itu sendiri.
2. Penyusunan DRP memerlukan studi awal untuk menentukan DRP yang paling optimal yang sesuai dengan kemampuan dan kebutuhan organisasi, serta manfaat yang diharapkan oleh organisasi dari DRP tersebut. Tingginya biaya dan usaha yang harus dilakukan oleh organisasi dalam penyusunan dan penerapan DRP membuat organisasi menghadapi kendala yang tidak ringan dan perlu penetapan skala prioritas yang tepat, sesuai dengan strategi bisnis dan kemampuan organisasi.
3. Studi kasus pada infrastruktur jaringan komputer Universitas Widyatama menghasilkan beberapa temuan yang kontradiktif yaitu tingginya tingkat kebergantungan para pengguna terhadap layanan jaringan komputer tetapi rendahnya tingkat pengetahuan pengguna dalam pengamanan data dari bencana. Pihak pengelola jaringan komputer universitas juga tidak memiliki rencana dan mekanisme yang jelas untuk menghadapi bencana, khususnya yang terkait dengan bencana skala kecil pada jaringan komputer seperti serangan virus, serangan hacker, kegagalan hardware atau gangguan infrastruktur seperti terputusnya listrik, kebakaran dan lain-lain.

DAFTAR PUSTAKA

[1] Falahah, "Pengembangan Model Perencanaan Penanggulangan Bencana (Disaster Recovery Plan) pada Sektor Teknologi Informasi", Tesis Magister Sistem Informasi, Program Studi Informatika, STEI, ITB, 2006.
[2] Gregory, Peter, CISA, CISSP, "IT Disaster Recovery Planning for Dummies", Willey Publishing, Inc, 2007.
[3] http://en.wikipedia.org/wiki/Disaster_recovery, diakses tanggal 16 Juni 2011.
[4] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41532 "ISO/IEC 24762:2008", diakses tanggal 16 Juni 2011.
[5] http://www.sysneta.com/memahami-firewall-dmz, diakses tanggal 16 Juni 2011.