Oleh: IRHAMNI ALI[1]
Email: *irhamni@Perpusnas.go.id*

Pengamanan Koleksi Digital dengan Pendekatan Manajemen Risiko

Abstrak

Teknologi menjadi bagian hidup manusia sehari-hari, kemajuannya menyebabkan terjadi ledakan informasi. Perpustakaan sebagai tempat pengelolaan informasi memperoleh dampak langsung dari perkembangan teknologi tersebut. Saat ini hampir sebagian besar perpustakaan menerapkan *hybrid library* atau perpustakaan campuran dimana sebagian koleksi dikemas dalam bentuk digital. Koleksi merupakan aset perpustakaan yang sangat berharga, karena itu penting dilakukan pengamanan terhadapnya, terutama pada era digital seperti sekarang ini yang mengakibatkan semakin beragamnya ancaman terhadap koleksi. Pendekatan manajemen risiko merupakan pendekatan untuk meminimalisasi risiko. Koleksi digital merupakan aset perpustakaan yang rentan terhadap risiko, pendekatan manajemen risiko akan memudahkan perpustakaan untuk mengidentifikasi risiko, mengevaluasi risiko untuk mengetahui konsekuensi, dan tindakan pilihan untuk meminimalisasi risiko serta tindakan prioritas dalam implementasi manajemen risiko dan pengembangan rencana manajemen risiko. Pada akhirnya semua elemen manajemen risiko yang telah disiapkan diharapkan tidak perlu dilaksanakan, karena tidak terjadi hal yang diinginkan dan risiko yang dihadapi tidak pernah terjadi**.**

Kata Kunci : *Manajemen Risiko, Koleksi Digital.*

Pendahuluan

Selama dua puluh tahun terakhir, perubahan cara pandang perpustakaan terhadap keandalan teknologi informasi dan komunikasi elektronik telah menghasilkan sarana baru dalam memberikan informasi kepada masyarakat, yaitu perpustakaan digital. Perpustakaan digital akan memudahkan pemustaka dalam mengakses informasi dalam bentuk digital. Pemenuhan kebutuhan informasi diharapkan dapat dilakukan secara akurat melalui representasi dalam bentuk digital tanpa paparan fisik ke sumber utama serta tanpa batas ruang dan waktu. Salah satu aset perpustakaan digital yang sangat penting adalah ketersediaan koleksi. Saat ini ketersediaan koleksi sering didefinisikan ulang sebagai kombinasi dari bahan perpustakaan yang direpresentasikan dalam bentuk elektronik guna memenuhi permintaan informasi berbasis teks atau visual dengan menggunakan konteks dan berfungsi sebagai kunci untuk menemukan mereka.

Aksesbilitas yang sangat cepat terhadap koleksi di perpustakaan pada era digital saat ini dapat mengakibatkan rentannya koleksi terhadap penyalahgunaan, pencurian, atau kerusakan. Untuk itu, sejumlah langkah perlu dilaksanakan untuk menjaga koleksi, antara lain pengendalian terhadap akses, pemilihan koleksi, pengolahan metadata pada koleksi, sampai pada diseminasi informasi melalui pemantauan administrasi hak dan rilis, dan prosedur yang ketat mengenai penggunaan oleh pemustaka, pustakawan. Koleksi digital sangat terpengaruh oleh tindakan yang dilakukan oleh pengelola data dan pengguna data untuk itu diperlukan langkah keamanan untuk melindungi aset ini (Teresa, 1999).

Konsep manajemen risiko mulai diperkenalkan di bidang keselamatan dan kesehatan kerja pada era tahun 1980-an setelah berkembangnya teori ***accident model*** dari ILCI seiring dengan semakin maraknya isu lingkungan dan kesehatan. Manajemen risiko bertujuan untuk minimisasi kerugian dan meningkatkan kesempatan ataupun peluang termanfaatkannya

[1] Perencana Pertama Perpustakaan Nasional RI

sumberdaya selama-mungkin dan seefisien mungkin. Jika terjadi kerugian manajemen risiko dapat memotong mata rantai kerugian tersebut, sehingga efek dominonya tidak akan terjadi pada institusi secara menyeluruh. Pada dasarnya manajemen risiko bersifat pencegahan terhadap terjadinya kerugian maupun '*accident*'.

Manajemen risiko di perpustakaan merupakan studi komprehensif dan membutuhkan analisa mengenai munculnya potensi bahaya yang dapat berubah menjadi risiko jika langkah-langkah tidak diambil perpustakaan, sebagai contoh adalah risiko yang mungkin dapat menyebabkan kerusakan pada bangunan serta koleksinya. Manajemen risiko di perpustakaan lebih banyak ditujukan kepada langkah-langkah untuk mengurangi risiko tersebut secara teratur. Saat ini banyak rekomendasi mengenai penilaian risiko untuk mengurangi risiko di perpustakaan. Salah satunya adalah dari IFLA yang merekomendasikan anggotanya untuk mengurangi risiko dari bencana alam, konflik, dan krisis (IFLA,2012). IFLA mendorong dilakukan pengamanan untuk menghormati kekayaan budaya, terutama dengan meningkatkan kesadaran, mempromosikan manajemen risiko bencana, serta memperkuat kerjasama dan partisipasi dalam menjaga warisan budaya melalui UNESCO.

Tulisan ini dibuat untuk mengidentifikasi masalah risiko pada koleksi digital dan bagaimana penilaian risiko terhadap koleksi digital dari peluang risiko yang mungkin terjadi melalui pendekatan standar manajemen risiko. Metode pendekatan menajemen risiko merupakan metode yang tersusun secara logis dan sistematis dari suatu rangkaian kegiatan: penetapan konteks, identifikasi, analisa, evaluasi, pengendalian serta komunikasi risiko.

Manajemen Resiko

Manajemen risiko adalah sejumlah kegiatan yang diarahkan dan diterima untuk mengakomodasi kemungkinan kegagalan dalam program. Manajemen risiko didasarkan pada penilaian, setiap penilaian manajemen risiko mencakup tindakan sebagai berikut :

1. identifikasi risiko,
2. evaluasi risiko untuk kemungkinan dan konsekuensi,
3. penilaian pilihan untuk menampung risiko,
4. prioritas upaya manajemen risiko, dan
5. pengembangan rencana manajemen risiko

Manajemen risiko merupakan bagian yang tidak terpisahkan dari manajemen proses. Manajemen risiko adalah bagian dari proses kegiatan di dalam organisasi dan pelaksananya terdiri dari mutlidisiplin keilmuan dan latar belakang, manajemen risiko adalah proses yang berjalan terus menerus. Elemen utama dari proses manajemen risiko, meliputi:

1. Penetapan tujuan
   Menetapkan strategi, kebijakan organisasi dan ruang lingkup manajemen risiko yang akan dilakukan.
2. Identifikasi risiko
   Mengidentifikasi apa, mengapa dan bagaimana faktor-faktor mempengaruhi terjadinya risiko untuk analisis lebih lanjut.
3. Analisis risiko
   Dilakukan dengan menentukan tingkatan probabilitas dan konsekuensi yang akan terjadi. Kemudian ditentukan tingkatan risiko yang ada dengan mengalikan kedua variabel tersebut (probabilitas X konsekuensi).
4. Evaluasi risiko
   Membandingkan tingkat risiko yang ada dengan kriteria standar. Setelah itu tingkatan risiko yang ada untuk beberapa *hazards* dibuat tingkatan prioritas manajemennya. Jika tingkat risiko ditetapkan rendah, maka risiko tersebut masuk ke dalam kategori yang dapat diterima dan mungkin hanya memerlukan pemantauan saja tanpa harus melakukan pengendalian.
5. Pengendalian risiko
   Melakukan penurunan derajat probabilitas dan konsekuensi yang ada dengan menggunakan berbagai alternatif metode, bisa dengan transfer risiko, dan lain-lain.
6. *Monitor* dan *Review*
   Monitor dan *review* terhadap hasil sistem manajemen risiko dilakukan serta mengidentifikasi perubahan-perubahan yang perlu dilakukan.
7. Komunikasi dan konsultasi
   Komunikasi dan konsultasi dengan pengambil keputusan internal dan eksternal

Manajemen risiko dapat diterapkan di setiap level organisasi. Manajemen risiko dapat diterapkan di level strategis dan level operasional. Manajemen risiko juga dapat diterapkan pada proyek yang spesifik, untuk membantu proses pengambilan keputusan ataupun

untuk pengelolaan daerah dengan risiko yang spesifik. Manajemen risiko adalah sesuatu yang tidak pasti, perpustakaan juga membutuhkan analisis risiko untuk peramalan ketidakpastian tersebut. Sebagai soal fakta, ketika risiko terjadi, itu akan menyebabkan efek negatif pada perpustakaan (Kuzucuoglu, 2014). Risiko tersebut harus proaktif diidentifikasi. Risiko memiliki 2 parameter utama, yaitu:

1. Probabilitas terjadinya risiko,
2. Dampak dari risiko yang terjadi, dan pasti harus menunjukkan hasil (seperti kerusakan / kerugian).

Manajemen Resiko Koleksi Digital

Praktik manajemen risiko pada koleksi digital haruslah menjadi bagian integral dari pelaksanaan sistem manajemen perpustakaan digital. Proses manajemen risiko merupakan salah satu langkah yang dapat dilakukan untuk terciptanya sistem yang berkelanjutan. Proses manajemen risiko koleksi digital juga harus bisa membantu dalam proses pengambilan keputusan dalam mengembangkan koleksi perpustakaan. Manajemen risiko koleksi digital didasarkan pada elemen-elemen manajemen risiko, sebagai berikut :

1. Penetapan tujuan
   Menetapkan strategi, kebijakan organisasi dan ruang lingkup manajemen risiko yang akan dilakukan khususnya pada koleksi digital yang dimiliki oleh perpustakaan.

2. Identifikasi risiko pada koleksi digital
   Proses ini meliputi identifikasi risiko pada koleksi digital dengan melihat pada segala kemungkinan yang terjadi terhadap semua risiko yang mungkin terjadi sebanyak mungkin secara akurat dan komplit. Teknik yang dapat digunakan dalam identifikasi risiko antara lain:
   a. Brainstorming dengan penyedia koleksi digital
   b. Survei dengan pemustaka
   c. Wawancara pustakawan
   d. Informasi historis koleksi digital

3. Analisis risiko pada koleksi digital
   Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah melakukan analisa potensial terjadinya risiko pada koleksi digital yang dimiliki perpustakaan dengan melihat seberapa besar *severity* (kerusakan) dan probabilitas terjadinya risiko tersebut. Risiko pada koleksi digital biasanya berkaitan erat dengan sistem informasi yang digunakan oleh perpustakaan, hal ini berkaitan erat dengan *cybercrime* di perpustakaan digital (Ali, 2011), risiko yang dihadapi oleh koleksi digital antara lain:

a. Data thief (pencurian)
   Data thief atau pencurian data merupakan bentuk kejahatan yang sering terjadi. Hal ini harus diantisipasi oleh para pustakawan dengan upaya meminimalisasi kemungkinan para pelaku *cybercrime* untuk melakukan pencurian. Dalam ranah perpustakaan digital pencurian data bisa dikategorikan sebagai *data Leakage*, yaitu menyangkut bocornya data pemustaka atau data lainnya ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa nama, kontak serta kebiasaan pemustaka dalam memakai koleksi perpustakaan. Hal ini berbahaya jika jatuh ke tangan yang salah sehingga bisa digunakan untuk sesuatu yang tidak diinginkan seperti pelanggaran privasi pemustaka yang apabila diketahui oleh orang lain maka dapat merugikan pemustaka secara materil maupun imaterial.

   Jika data yang dicuri merupakan koleksi perpustakaan yang berbentuk digital maka hal ini masuk dalam kategori *Offense Against Intellectual Property,* yaitu kejahatan yang ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Hal tersebut sangat berbahaya bagi perpustakaan karena koleksinya dapat diakses keluar dan di perdagangkan secara ilegal dan jika hal ini terjadi maka bukan hanya pihak perpustakaan saja yang dirugikan namun juga pihak pengarang sebagai pemilik hak kekayaan intelektual (Gollese, 2006).

b. Joy computing, yaitu pemakaian komputer orang lain tanpa izin, termasuk penggunaan program komputer, password komputer, kode akses, atau data sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah,

intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain. Hal ini biasanya terjadi pada OPAC perpustakaan dimana OPAC digunakan sebagai sarana untuk menyebarkan virus atau digunakan sebagai host untuk mengakses ke server tanpa izin, untuk itu pustakawan perlu memikirkan cara agar OPAC yang ada di perpustakaan tidak disalahgunakan oleh pemustaka untuk tindakan *Joy Computing*.

c. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal bisa dari dalam perpustakaan dengan menggunakan OPAC atau dari luar perpustakaan dengan memanfaatkan port yang terbuka, hacking biasanya bertujuan untuk *defacing* dan *cracking*. *Defacing* merupakan aktivitas seorang hacker untuk melakukan perubahan tampilan pada web perpustakaan, biasanya pelaku *defacing* hanya bertujuan untuk mengetes ilmu atau unjuk kemampuan diantara sesama hacker, sementara *cracker* bertujuan untuk menganggu jaringan komunikasi data, dan melakukan penetrasi jaringan sistem komputer untuk melakukan pencurian data, serta bertujuan membuat sistem gagal berfungsi yang mengakibatkan *Frustating data communication* atau penyia-nyiaan data komputer. Hal ini biasanya dilakukan dengan serangan DoS *(Denial Of Service)* dimana server gagal berfungsi karena terlalu banyak perintah yang masuk (Suheimi, 1995).

d. *Data diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data, atau output data. Biasanya hal ini terjadi pada bagian sirkulasi dimana pihak-pihak tertentu berusaha untuk mengubah data peminjaman atau merubah data tertentu lainnya. Kejadian seperti ini perlu diantisipasi oleh pustakawan agar tidak terjadi kehilangan data atau *data loss.*

e. *Electronic mutilation* dan *data vandalism*
Electronic mutilation dan *data vandalism* muncul sebagai akibat dari menjamurnya komunitas maya dan kemudahan akses berkomunikasi melalui internet (Suheimi, 1995). Modus yang dilakukan adalah: masuk ke sebuah database dengan terlebih dahulu melumpuhkan sistem keamanan database tersebut, kemudian melakukan sabotase terhadap data yang mereka perlukan sehingga data tersebut menjadi rusak dan tidak bisa dipergunakan kembali. Namun Hacker bukanlah salah satu ancaman dari e*lectronic mutilation* dan *data vandalism* karena masih terdapat beberapa ancaman lainnya yakni:

- Ulat *(Worm)* merupakan program yang mempunyai kemampuan menggandakan diri namun tidak mempunyai kemampuan menempelkan dirinya pada suatu program. Dia hanya memanfaatkan ruang kosong pada memori komputer untuk menggandakan diri. Sehingga memori komputer akan menjadi penuh dan sistem komputer akan berhenti.
- *Bot* merupakan istilah bagi suatu bagian program komputer yang mempunyai kemampuan mengacau dan merusak sistem komputer berdasarkan kondisi yang telah diprogramkan di dalamnya.
- *Backdoor/Back office trap/*pintu Jebakan merupakan program yang mempunyai kemampuan melumpuhkan sistem pengamanan suatu komputer, sehingga pembuat program dapat keluar masuk sistem tanpa harus melalui sistem pengamanan normal yang ditetapkan pada suatu sistem komputer.
- *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain. Biasanya Program Trojan berfungsi sebagai kamuflase dari virus tidak merusak. Namun sisipan program di dalamnya patut diwaspadai karena menyerang sistem operasi, directory dan *boot record*.

- Virus (Komputer) merupakan program kecil yang dapat memperbanyak dirinya sendiri. Virus merusak secara berlahan-lahan *boot record*, sistem operasi, dan directory bahkan bisa merusak fisik suatu media penyimpanan (Andi, 1990).

4. Evaluasi risiko pada koleksi digital
   Evaluasi risiko bertujuan untuk menentukan dugaan yang terbaik agar perpustakaan mampu memprioritaskan dengan baik dalam implementasi perencanaan manajemen risiko. Tahap ini juga bertujuan untuk mengukur apakah kemungkinan risiko akan terwujud? Apakah perpustakaan sudah menggunakan langkah-langkah aktif maupun pasif untuk mencegah atau meminimalkan dampak dari risiko yang dihadapi.

   Evaluasi risiko juga perlu membandingkan tingkat risiko yang ada dengan kriteria standar. Setelah itu tingkatan risiko yang ada untuk beberapa *hazards* dibuat tingkatan prioritas manajemennya. Jika tingkat risiko ditetapkan rendah, maka risiko tersebut masuk ke dalam kategori yang dapat diterima dan mungkin hanya memerlukan pemantauan saja tanpa harus melakukan pengendalian.

5. Pengendalian risiko koleksi digital
   Tulang punggung perpustakaan adalah aset informasi yang berkolaborasi dengan perangkat teknologi informasi dan jaringan global dengan sistem informasi manajemen perpustakaan sebagai pintu masuk utama memberikan layanan kepada pemustaka. Namun demikian permasalahan aset informasi perpustakaan dengan basis teknologi informasi ternyata masih diabaikan oleh perpustakaan itu sendiri, padahal apabila terjadi kerusakan dalam pengelolaan aset informasi tersebut layanan perpustakaan menjadi terhenti dan tidak berjalan maksimal.

   Perpustakaan sudah seharusnya mengantisipasi berbagai macam kendala yang dapat menghambat berjalannya sistem layanan perpustakaan yang biasanya disebut sebagai sebuah risiko atau kejadian yang seharusnya dihindari dalam kegiatan perpustakaan. Manajemen risiko koleksi digital harus bisa memberi jawaban dan solusi sehingga risiko dapat dikaji dan mampu meminimalkan efek negatif dari risiko pada tingkat yang dapat diterima.

6. *Monitor* dan *Review*
   Manajemen risiko merupakan proses yang *sustainable* atau proses yang terus menerus dilakukan karena perkembangan teknologi terus berkembang dengan pesat. Untuk itu *Monitor* dan *review* terhadap hasil sistem manajemen risiko yang dilakukan serta mengidentifikasi perubahan-perubahan perlu dilakukan.

7. Komunikasi dan konsultasi
   Ketika risiko telah terjadi perpustakaan perlu melakukan komunikasi dan konsultasi dengan pengambil keputusan internal dan eksternal (konsultan, *stakeholder*) untuk bisa langsung menindaklanjuti hasil manajemen risiko yang dilakukan.

Penutup

Manajemen risiko harus dikembangkan berdasarkan sifat unik dari koleksi digital masing-masing lembaga serta tipe pemustaka yang mengaksesnya. Hal ini perlu diterapkan mengingat bahwa tujuan dari manajemen risiko yaitu untuk meminimalisasi kegagalan yang diterima lembaga. Lembaga juga harus mengantisipasi risiko dengan memiliki sumber daya untuk membuat, menyimpan, dan menggunakan koleksi digital yang sesuai standar keamanan saat ini. Hal ini perlu agar manajemen risiko beserta para elemennya tidak perlu dilaksanakan, karena tidak terjadi hal-hal yang diinginkan dan risiko yang dihadapi tidak pernah terjadi.

Daftar Pustaka

Ali, I. (2011). *Kejahatan Terhadap Informasi (Cybercrime) Dalam Konteks Perpustakaan Digital.* http://hdl.handle.net/10760/16968 Akses tanggal 19 Februari 2016].

Andi, H. (1990). *Aspek-aspek Pidana di Bidang Komputer*. Jakarta : Sinar Grafika.

Beamsley, T.G. (1999). Securing digital image assets in museums and libraries: A risk management approach. *Library Trends*, 48 (2): 359-378.

Gollese, P.R. (2006). Perkembangan cybercrime dan upaya penanganannya di Indonesia oleh polri. *Buletin Hukum Perbankan dan kebanksentralan*, Vol 4 (2) Agustus 2006.

The International Federation of Library Associations and Institutions (IFLA). (2011). http://www.ifla.org/strategic-plan/key-initiatives/2011-2012 [Akses tanggal 24 Mei 2016].

Kenney, A.R. & McGovern, N. (2002). Preservation risk management for Web resources. *Information Management Journal,* 36 (5) Sep/Oct 2002: 52-61.

Kuzucuoglu, A.H. (2014). Risk Management In Libraries, Archives And Museums. *IIB International Refereed Academic Social Sciences Journal,* 5(15), 277-294. Retrieved from http://search.proquest.com/docview/1647083539?accountid =25704 [Akses tanggal 23 Mei 2016].

Nurrohman, A. *(*2012). *Manajemen Risiko Sistem Informasi Manajemen Perpustakaan.* http://arifnurblog.blogspot.com/2012/07/manajemen-risiko-sistem-informasi.html [Akses tanggal 19 februari 2016].

Pinontoan, J.H. (2010). "Manajemen Risiko TI – Konsep-konsep". *Majalah PC Media*. Oktober 2010.

Sinaga, D. (2004). "Kejahatan Terhadap Buku dan Perpustakaan". *Visi Pustaka*, Vol 1 (6) Juli 2004.

Suheimi. (1995). Kejahatan Komputer. *Visi Pustaka*, Vol. 14 (1).

Sulistyo-Basuki. (2011). Bahan Kuliah Perpektif Ilmu Perpustakaan dan Informasi. Bogor: Institut Pertanian Bogor.

Sulistyo-Basuki. (1994). *Pengantar Ilmu Perpustakaan*. Jakarta : Gramedia.

Teresa, G. B. (1999). Securing digital image assets in museums and libraries: A risk management approach. *Library* Trends, 48(2), 359-378. Retrieved from http://search.proquest.com/docview/220438439?accountid=25704