IJM: Indonesian Journal of Multidisciplinary
e-ISSN: 3025-5961
Volume 3 Nomor 1 Tahun 2025
https://ojs.csspublishing.com/index.php/ijm

Implementasi Manajemen *Security* Terhadap *Cyber Attack*

Daniel Fernando S Laia[1], Nurfiyah[2]
Universitas Bhayangkara Jakarta Raya[1,2]
e-mail: dfernandoslaia@gmail.com

Abstract
The development of Information Technology (IT) is a major asset in the sustainability of an organization, both private and government companies. This can open up opportunities for increased cybercrime that can be dangerous and cause losses, so that anticipatory steps and strengthening of security management are needed. Information security is a method used to provide protection and secure data, information and information systems from activities that can change, damage or delete data without authorized authority. Security management is responsible for identifying and analyzing information security risks, securing systems and networks to remain protected from cyber attacks that can endanger and harm the company. Cybersecurity is an effort to protect computer systems, networks, software, and data from attacks, unauthorized access, changes, or destruction by unauthorized parties. This study was conducted using a descriptive qualitative method, namely collecting and analyzing data on the definition of cybercrime, types of cybercrime and implementation of security management. The results of this study can provide an overview of cybercrime and security management as anticipatory steps against cyber attacks, especially in companies in Indonesia. The results of this study can also be a reference in improving security in information systems from cybercrime threats.
Keywords: *Security, Cyber, Information*

Abstrak
Perkembangan Teknologi Informasi (TI) merupakan aset utama dalam keberlangsungan suatu organisasi baik perusahaan swasta maupun pemerintah. Hal ini dapat membuka peluang pada peningkatan kejahatan *cybercrime* yang dapat membahayakan dan menyebabkan kerugian, sehingga perlu adanya langkah antisipasi dan penguatan manajemen kemanan. Keamanan informasi adalah metode yang digunakan untuk memberikan perlindungan dan mengamankan data, informasi dan sistem informasi dari kegiatan yang dapat mengubah, merusak atau menghapus data tanpa otoritas yang telah diizinkan. Manajemen sekuriti bertanggung jawab untuk mengidentifikasi dan menganalisis risiko keamanan informasi, mengamankan sistem dan jaringan agar tetap terlindungi dari serangan *cyber* yang dapat membahayakan dan merugikan perusahaan. *Cybersecurity* atau keamanan siber adalah upaya untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari serangan, akses yang tidak sah, perubahan, atau penghancuran oleh pihak yang tidak berwenang. Penelitian ini dilakukan dengan metode kualitatif deskriptif yaitu mengumpulkan dan menganalisis data mengenai definisi *cybercrime*, jenis-jenis *cybercrime* dan implementasi manajemen *security*. Hasil dari penelitian ini dapat memberikan gambaran mengenai *cybercrime* dan manajemen *security* sebagai langkah antisipasi terhadap serangan *cyber*, khususnya pada perusahaan di Indonesia. Hasil penelitian ini juga dapat menjadi acuan dalam meningkatkan keamanan pada sistem informasi dari ancaman *cybercrime.*
Kata Kunci: Keamanan, Siber, Informasi

PENDAHULUAN

Perkembangan Teknologi Informasi (TI) saat ini telah mengalami kemajuan pesat dan menjadi kebutuhan utama bagi seluruh organisasi perusahaan baik swasta maupun pemerintah. TI berperan penting sebagai penunjang dalam efisiensi dan evektifitas peningkatan kinerja. Oleh karena itu, perlu pengelolaan yang baik dalam teknologi informasi karena didalamnya terdapat informasi penting yang menjadi aset organisasi perusahaan. Apabila terjadi insiden, maka dapat berpengaruh terhadap keberlangsungan bisnis dan mengakibatkan kerugian bagi perusahaan (Nasher, 2018). Teknologi informasi dan komunikasi merupakan aset yang penting bagi perseorangan, perusahaan swasta maupun instansi pemerintahan. Semakin banyak instansi yang menggunakan teknologi infomasi maka informasi yang harus dikelola juga semakin banyak. Informasi merupakan sekumpulan data yang dikelompokkan dan diinterpretasikan untuk digunakan dalam proses pengambilan keputusan. Oleh karena itu, informasi adalah aset yang sangat penting dan harus dilindungi untuk mencegah penyalahgunaan informasi tersebut (Ramadhani *et al*., 2020)

Penggunaan teknologi informasi dimanfaatkan untuk memberikan akses yang cepat dan mudah serta jangkauan yang sangat luas. Perkembangan teknologi informasi juga menimbulkan berbagai permasalahan keamanan data bagi penggunanya. Perlindungan sistem informasi biasanya dikenal dengan sistem kontrol dan keamanan untuk melindungi aset TI dari gangguan yang disengaja maupun tidak disengaja. Keamanan informasi perlu diperhatikan karena penyalahgunaan akses data dapat menyebabkan dampak negatif yang berbahaya. Keamanan informasi adalah aset yang sangat berharga yang meliputi kebijakan, prosedur, proses dan kegiatan dengan tujuan untuk melindungi informasi. Informasi penting harus dijaga dan dilingkungi dari berbagai ancaman, baik dari internal maupun eksternal. Sistem informasi adalah seperangkat fungsi manajemen operasional yang mampu membuat keputusan dengan tepat, cepat dan sistematis (Novianto *et al.,* 2023).

Keamanan informasi merupakan metode yang digunakan untuk melindungi data, informasi dan sistem informasi dari kegiatan yang dapat mengubah, merusak atau menghapus data tanpa otoritas yang telah diizinkan sehingga dapat membahayakan dan merugikan pemilik data tersebut (Yunella, *et al.* 2019). Manajemen sekuriti bertanggung jawab untuk mengidentifikasi dan menganalisis risiko keamanan informasi, mengamankan sistem dan jaringan agar tetap terlindungi dari serangan *cyber* yang dapat membahayakan dan merugikan perusahaan. *Cybersecurity* atau keamanan siber adalah upaya untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari serangan, akses yang tidak sah, perubahan, atau penghancuran oleh pihak yang tidak berwenang. *Cybersecurity* melibatkan teknologi, kebijakan, dan praktik-praktik yang dirancang untuk melindungi komputer, jaringan, dan

sistem informasi dari berbagai jenis ancaman siber, termasuk serangan *malware, phishing*, dan serangan *denial-of-service* (DoS) (Soesanto *et al.,* 2023).

Cybercrime merupakan serangkaian kegiatan kriminal yang melibatkan teknologi komputer, jaringan dan sisitem informasi. Penggunaan jaringan global telah membuka peluang bagi para penjahat siber untuk dapat melakukan serangannya hingga melintasi seluruh dunia tanpa terbatas jarak dan waktu. Kejahatan cyber meliputi berbagai tindakan seperti pencurian data (*skimming*), peretasan (*hacking*) dan *software* berbahaya (*malware*). Kerugian akibat *cybercrime* sulit diperkirakan karena selain mengakibatkan kerugian finansial, *cybercrime* juga mengakibatkan kerusakan, kehilangan dan bocornya data pribadi yang dapat menurunkan reputasi perusahaan. Berdasarkan data Badan Siber dan Sandi Negara (BSSN) anomali trafik atau serangan siber yang ada di Indonesia sepanjang tahun 2022 adalah sebanyak 714.170.967 serangan. Oleh karena itu, permasalahan *cyber crime* harus diperhatikan agar tidak membahayakan dan menimbulkan kerugian semakin banyak (Sufi *et al.,* 2023)

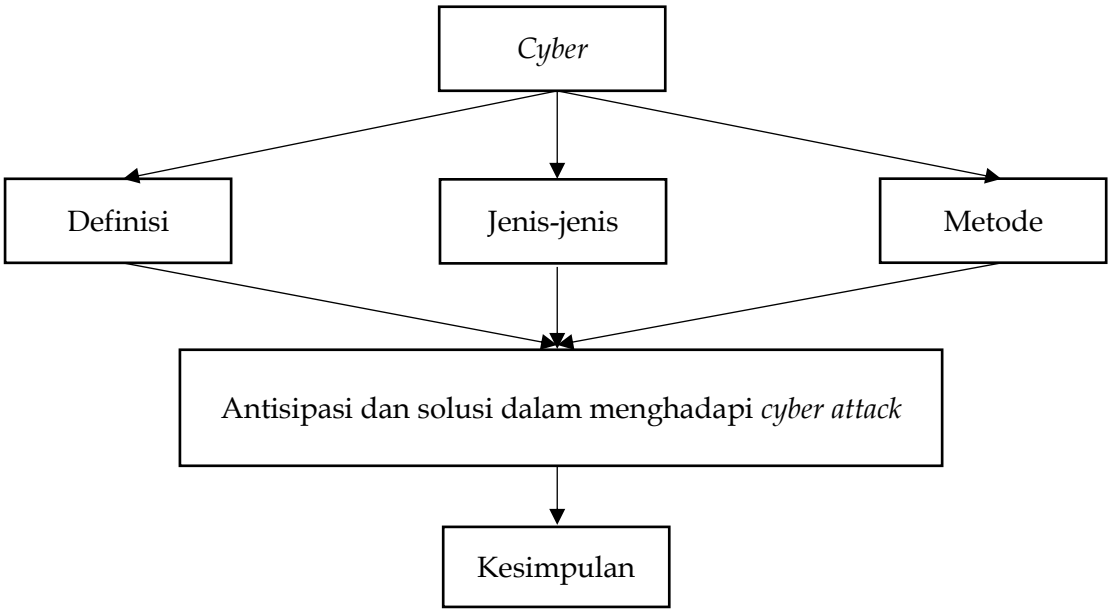
Berbagai kejahatan *cyber* yang terjadi di Indonesia memberikan bukti bahwa ancaman tersebut harus diwapadai dengan cara melindungi data dan informasi sebaik mungkin. Selain itu, perlunya antisipasi dalam menghadapi serangan *cyber* yang dapat membahayakan dan merugikan perusahaan. Penelitian ini dilakukan dengan mengumpulkan, memilih dan menganalisis data mengenai definisi *cybercrime*, jenis-jenis *cybercrime* dan implementasi manajemen *security*. Hasil penelitian ini dapat memberikan penjelasan mengenai *cyber* dan manajemen *security* sebagai langkah antisipasi terhadap serangan *cyber* pada perusahaan di Indonesia. Selain itu, hasil penelitian dapat digunakan sebagai acuan dalam meningkatkan keamanan sistem informasi di perusahaan dari ancaman *cybercrime*.

METODE PENELITIAN

Metode Penelitian yang digunakan dalam penelitian ini adalah kualitatif dengan pendekatan deskriptif yaitu mengumpulkan dan menganalisis data yang berkaitan dengan penelitian agar dapat ditarik kesimpulan yang menggambarkan suatu fenomena. Penelitian kualitatif merupakan penelitian yang sangat tepat untuk menjawab permasalahan yang kompleks. penelitian kualitatif mengacu pada pendekatan penelitian yang menghasilkan data deskriptif. Data tersebut bersumber dari hasil pengamatan baik tertulis, lisan atau perilaku dari subjek penelitian. adapun data deskriptif terbentuk dari hasil eksplorasi dan pemaknaan peneliti terhadap topik yang diteliti. Penelitian kualitatif adalah metode yang penelitian yang menekankan pada pengamatan dan pemahaman secara alamiah dan mendalam, disajikan secara deskriptif dan diinterpretasikan secara komprehensif. Penelitian kualitatif deskriptif didefinisikan sebagai metode yang digunakan untuk menemukan pengetahuan

atau teori mengenai topik tertentu. Pada proses pengkajian, peneliti akan mencari kesamaan atau menemukan ketidaksamaan, memberikan pandangan, meringkas dan menggabungkan suatu teori menjadi sebuah pemikiran baru guna menjawab permasalahan yang diteliti (Waruwu, 2024).

Penulis akan menggunakan metode kualitatif deskriptif untuk mendeskripsikan hasil analisis mengenai Implementasi Manajemen *Security* Terhadap *Cyber Attack,* khususnya pada perusahaan di Indonesia. Peneliti menggunakan jenis penelitian kualitatif untuk memperoleh data yang dibutuhkan secara jelas dan spesifik. Teknik yang digunakan untuk mengumpulkan data yaitu triangulasi (gabungan) dan analisis data secara kualitatif. Berikut adalah metodologi yang digunakan dalam penelitian ini:



Gambar 1. Kerangka Penelitian

PEMBAHASAN

Cybercrime adalah sekelompok aktivitas yang dilakukan dengan menciptakan gangguan pada jaringan informasi, mencuri data penting milik pribadi, perusahaan atau instansi pemerintah, meretas rincian dan mengambil kekayaan. *Cybercrime* merupakan tindakan ilegal yang dilakukan dengan penjahat yang menggunakan teknologi sistem informasi jaringan komputer untuk secara langsung menyerang teknologi sistem informasi korbannya. *Cybercrime* juga dapat diartikan sebagai kegiatan kriminal yang menggunakan teknologi komputer berupa internet sebagai alat utama kejahatannya dan merupakan salah satu bentuk kegiatan kriminal yang melanggar hukum. *Cyber crime* menjadi ancaman serius yang dapat merusak kepentingan individu, perusahaan, bahkan negara, sehingga membutuhkan *cyber security* untuk melindungi sistem

komputer dari berbagai serangan dan akses ilegal yang dapat menganggu keamanan data dan informasi pada jaringan. Hal ini termasuk menjaga sistem dari akses tidak sah, mencegah serangan jahat, serta memastikan keamanan dan integritas data (Gunawan *et al.*, 2024)

Dalam *cyber attack*, terdapat istilah *malware* yaitu setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses dan menyebabkan bahaya dan kerusakan *system*. Selain virus, terdapat beberapa jenis serangan *malware* antara lain adalah (1) *Spyware* yang melacak aktivitas, pengumpulan penekanan tombol, dan pengambilan data, (2) *Adware*, untuk menampilkan iklan yang juga membawa spyware, (3) *Bot*, secara otomatis menjalankan tindakan tertentu secara *online*, (4) *Ransomware*, mengenkripsi data di komputer dengan kunci yang tidak diketahui penggunanya. Jenis-jenis *malware* tersebut yang dimanfaatkan untuk mempengaruhi karakteristik ruang siber. *Cyber attack* juga dapat memuat konten ilegal seperti dokumen elektronik yang melanggar seperti kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan, pengancaman, penyebaran *hoax* yang menyesatkan dan ancaman kekerasan (Budi *et al.*, 2021).

Jenis-jenis *cybercrime* yang sering ditemukan pada aktivitas dunia maya, antara lain adalah (Soesanto *et al.*, 2023), cybercrime atau kejahatan dunia maya mencakup berbagai jenis tindak kejahatan yang dilakukan melalui internet. Salah satu jenisnya adalah kejahatan yang terkait dengan e-commerce dan website perusahaan, di mana aktivitas perdagangan daring seperti promosi, transaksi, dan pembayaran dapat dimanfaatkan untuk melakukan kejahatan seperti pemalsuan kartu kredit, persaingan tidak sehat, monopoli barang, serta pelanggaran hak kekayaan intelektual (HaKI). Selain itu, terdapat juga cybersex, yaitu dunia pornografi yang dapat diakses secara bebas atau berbayar melalui internet, yang sering kali melibatkan pengguna di bawah umur. Kejahatan lainnya adalah hacking, di mana seorang hacker mengakses jaringan informasi tanpa izin dengan tujuan merusak atau mengubah data yang ada, sehingga menimbulkan kerusakan pada jaringan dan penyalahgunaan informasi. Cyber terrorism merupakan bentuk kejahatan yang sangat merugikan negara, di mana pelaku melakukan serangan terhadap komputer, jaringan, dan sistem informasi suatu negara untuk mengintimidasi pemerintah dan memaksakan kepentingan tertentu. Selain itu, penipuan melalui OTP (One Time Password) juga menjadi salah satu ancaman, di mana kode rahasia yang dikirimkan kepada pengguna dapat dicuri dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Phishing adalah jenis penipuan lain yang bertujuan untuk mencuri data pribadi korban, seperti nama, alamat, dan informasi keuangan, dengan menggunakan teknik penipuan untuk memperoleh informasi tersebut secara ilegal.

Manajemen *security* diperlukan untuk menangani dan menjaga keamanan informasi yang tersimpan dalam sistem agar tidak disalahgunakan. Manajemen sekuriti terdiri dari dua kata yaitu manajemen dan sekuriti, dimana manajemen artinya mengelola yang meliputi empat fungsi yaitu merencanakan, mengorganisasikan, melaksanakan dan mengarahkan atau mengontrol, sedangkan sekuriti adalah keamanan secara menyeluruh. Oleh karena itu, manajemen sekuriti merupakan serangkaian aktivitas keamanan yang terintegrasi mulai dari perencanaan, pengorganisasian, pelaksanaan dan pengawasan/pengendalian. Manajemen sekuriti adalah langkah yang dilakukan untuk mengamankan dan mencegah terjadinya kejahatan yang dapat merugikan dan menganggu operasional perusahaan (Nova *et al.*, 2023).

Keamanan informasi adalah upaya yang dilakukan untuk melindungan dan mengamankan aset informasi melalui beberapa jenis media seperti komputer, mesin fax dan fasilitas pendukung penyimpanan data seperti dokumen *hardcopy* dari berbagai ancaman yang dapat membahayakan. Manajemen keamanan informasi memiliki empat tahapan antara lain adalah (Hartati, 2017), Proses manajemen keamanan informasi dalam sebuah perusahaan melibatkan beberapa langkah penting. Langkah pertama adalah identifikasi ancaman, yang dapat berasal dari faktor internal maupun eksternal perusahaan. Proses ini penting dilakukan untuk memahami potensi risiko yang dapat membahayakan keamanan aset perusahaan. Setelah ancaman diidentifikasi, langkah selanjutnya adalah mengidentifikasi risiko yang mungkin timbul akibat ancaman tersebut, seperti pencurian, penyalahgunaan informasi, atau modifikasi data yang dapat merugikan perusahaan. Selanjutnya, perusahaan perlu menetapkan kebijakan keamanan informasi yang jelas. Kebijakan ini berfungsi sebagai pedoman untuk mengarahkan seluruh program keamanan, yang bertujuan untuk melindungi aset perusahaan dari ancaman yang ada. Terakhir, penerapan kontrol yang tepat menjadi langkah penting untuk menangani risiko yang telah diidentifikasi. Kontrol ini berfungsi untuk melindungi perusahaan dari ancaman yang dapat terjadi serta mengurangi dampak dari potensi insiden keamanan yang mungkin timbul.

Penelitian kualitatif adalah metode penelitian dengan menggunakan data deskriptif berupa bahasa tertulis atau lisan dari pelaku yang dapat diamati. Pendekatan kualitatif bertujuan untuk menjelaskan dan menganalisis fenomena tertentu. Penelitian kualitatif akan membantu memperoleh jawaban atau kesimpulan yang lebih terperinci dan memberikan makna mendalam pada objek yang diamati. Sehingga, penelitian kualitatif membutuhkan waktu yang relatif lebih lama dalam melakukan analisis data daripada penelitian kuantitatif (Saputra *et al.,* 2024).

Berdasarkan informasi yang telah dikumpulkan, diketahui bahwa serangan *cyber* yang paling sering terjadi pada perusahaan adalah *ransomware, craking, pishing* dan *hacking* yang terjadi pada system perusahaan maupun karyawan melalui email perusahaan. Akibatnya, *system* perusahaan mengalami kelumpuhan total dan tidak dapat beroperasi secara normal. Oleh karena itu, perlu adanya peningkatan *cyver security* secara masif pada seluruh aspek utamanya system informasi dan teknologi perusahaan (Soesanto *et al*., 2023).

Manajemen Sekuriti adalah pendekatan secara holistik yaitu kombinasi atas strategi, kebijakan, prosedur, teknologi, pendidikan dan pengawasan untuk memberikan keamanan dan perlindungan pada aset penting dari berbagai ancaman dan risiko keamanan. Pengendalian akses merupakan bagian penting dalam manajemen *security*, yang memastikan bahwa hanya pihak yang memiliki otoritas yang dapat mengakses aset informasi. Hal ini melibatkan penggunaan otentikasi, otoritas berbasis peran, dan monitoring aktivitas pengguna. Selain itu, perusahaan dapat mengimplementasikan teknologi keamanan seperti *farewall*, antivirus, enkripsi dan deteksi intruksi untuk mencegah adanya kebocoran data dan informasi serta ancaman *cyber attack.* Pelatihan dan kesadaran menjadi komponen primer dalam manajemen sekuriti, agar karyawan memiliki pengetahuan dan kesadaran terkait ancaman keamanan, serta perlunya manajemen insiden agar perusahaan memiliki persiapan dalam menangani insiden keamanan secara efektif dan efisien (Azhari *et al.,* 2024).

Peran manajemen sekuriti di era digitalisasi sangat penting karena menjaga integritas informasi dari segala ancaman keamanan. Dengan menerapkan manajemen keamanan yang terpadu, maka perusahaan dapat mengurangi risiko keamanan yang mungkin dapat menyerang aset informasi penting. Adapun peran manajemen sekuriti antara lain adalah (Andini *et al.,* 2024), yaitu manajemen sekuriti memiliki peran penting dalam melindungi dan menjaga kelangsungan operasional perusahaan serta kepentingan nasional. Salah satunya adalah melindungi aset informasi perusahaan dari ancaman siber seperti pencurian data, malware, dan ransomware yang dapat menyebabkan kerugian finansial, reputasi, dan operasional. Selain itu, manajemen sekuriti juga berfungsi untuk membantu organisasi mematuhi peraturan yang berlaku, sehingga perusahaan dapat menghindari denda dan sanksi hukum. Di sisi lain, manajemen sekuriti juga berperan dalam meningkatkan ketahanan nasional dengan mengidentifikasi, menganalisis, dan merespons ancaman keamanan siber yang dapat membahayakan kepentingan negara. Upaya ini memerlukan kolaborasi antara pemerintah, sektor swasta, dan lembaga internasional untuk menciptakan lingkungan siber yang aman demi keberlangsungan negara.

Bagi perusahaan terdapat banyak ancaman *cyber crime* yang dapat terjadi, seperti pencurian data perusahaan, pegawai dan bahkan konsumen, sehingga dapat

merugikan pihak perusahaan baik secara finansial maupun operasional seperti dituntut oleh konsumen, bocornya informasi perusahaan dan turunnya reputasi perusahaan. Oleh karena itu, pentingnya *cyber security* untuk memberikan keamanan dan melindungi aset informasi perusahaan dari berbagai ancaman. Konsep dasar cyber security terdiri dari tiga unsur yaitu (Khotimah *et al*., 2022): *Confidentiality* (kerahasiaan), merupakan aturan yang membatasi akses yang dimiliki perusahaan agar informasi tersebut tidak dapat diakses oleh pihak lain, *Integrity* (integritas), memastikan data yang dimiliki perusahaan tetap konsisten, akurat dan dapat dipercaya, *Availability* (ketersediaan), ketersediaan perangkat keras, perangkat lunak dan jaringan yang harus dipelihara dan ditingkatkan performanya agar dapat melindungi data secara maksimal.

Adapun langkah antisipasi yang dapat dilakukan oleh perusahaan dalam menghadapi *cyber attack* adalah (Soesanto *et al*., 2023), yaitu untuk meningkatkan keamanan siber, perusahaan perlu memodifikasi dan memperbarui sistem keamanan secara berkala, termasuk pembaruan sistem operasi, instalasi perangkat lunak ICS, serta pemeriksaan rutin untuk memastikan antivirus dan perangkat lunak keamanan lainnya berfungsi optimal. Selain itu, perusahaan harus memantau titik akses jarak jauh (remote access point) dan port desktop protokol jarak jauh (RDP) yang tidak digunakan. Langkah-langkah keamanan yang lebih lanjut meliputi enkripsi end-to-end pada setiap perangkat guna menghindari pemalsuan serta melindungi dari serangan saluran samping (side-channel attack) yang dapat membahayakan kunci enkripsi. Penerapan prosedur otentikasi dan kontrol akses yang ketat juga penting untuk mencegah akses tidak sah baik oleh karyawan maupun perangkat lunak.

Pengujian penetrasi dan audit internal secara rutin harus dilakukan untuk mengidentifikasi kerentanannya, sehingga sistem operasional dapat terus diperbarui dan diamankan. Penting bagi perusahaan untuk menyediakan pelatihan kesadaran bagi karyawan untuk menghindari serangan siber, seperti phishing, serta menerapkan prinsip-prinsip cyber hygiene yang tepat guna menjaga keamanan informasi. Backup data juga harus dilakukan secara teratur dengan salinan cadangan yang dilindungi kata sandi dan disimpan secara offline agar tidak dapat diakses atau dimodifikasi tanpa izin. Membuat rencana pemulihan yang mencakup penyimpanan data penting di lokasi yang aman dan terpisah secara fisik adalah langkah penting lainnya untuk menjamin kelangsungan operasi perusahaan jika terjadi insiden. Keamanan password juga perlu diperhatikan dengan memastikan penggunaan sandi yang kuat, penerapan otentikasi multi-faktor (MFA), serta pembaruan sandi secara berkala untuk menghindari penggunaan ulang sandi yang sama di banyak akun. Selain itu, keamanan email harus ditingkatkan dengan menandai pesan yang datang dari luar organisasi dan menonaktifkan hyperlink yang tertera dalam email tersebut.

KESIMPULAN

Cybercrime dilakukan dengan menciptakan gangguan pada jaringan informasi, mencuri data penting milik pribadi, perusahaan atau instansi pemerintah, meretas rincian dan mengambil kekayaan. Jenis-jenis *cybercrime* yang banyak ditemui di dunia maya yaitu pada *e-commerce* atau *website* perusahaan, *cybersex, hacker, cyber terrorism, phising* dan penipuan OTP. Perlu adanya manajemen *security* yang kuat sebagai langkah antisipasi untuk menjaga keamanan informasi yang tersimpan dari serangan *cyber*. Terdapat beberapa langkah antisipasi dalam menghadapi *cyber attack* seperti memodifikasi dan memperbarui keamanan siber, melakukan enkripsi, menerapkan prosedur otentikasi dan akses kontrol, melakukan pengujian penetrasi dan audit internal, menyediakan pelatihan kesadaran atas bahaya *cyber attack*, melakukan *backup* data, membuat rencana pemulihan, memastikan keamanan *password* dan email. Implementasi manajemen *security* harus terus dievaluasi dan disempurnakan agar dapat memberikan manfaat yang signifikan dalam memberikan keamanan informasi dari serangan siber. Oleh karena itu, perusahaan di Indonesia perlu melakukan evaluasi mendalam pada manajemen *security* mulai dari implementasi kebijakan, pemantauan dan deteksi serta respons terhadap insiden keamanan. Hal ini dapat menjadi bahan pengambilan keputusan dalam penguatan manajemen security guna menghadapi *cyber attack*.

DAFTAR PUSTAKA

Andini, D. *et al*. (2024). Peranan Manajemen Sekuriti Terhadap Keamanan Cyber Bersumber Nilai-Nilai Kebangsaan UUD 1945 Dalam Meningkatkan Efektivitas di Era Digitalisasi Untuk Keamanan Nasional. *MENAWAN: Jurnal Riset dan Publikasi Ilmu Ekonomi*, *2*(3), pp.272–284.

Azhari, F. *et al*. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi *E-wallet. Jurnal Kewirausahaan dan Multi Talenta (JKMT)*, *2*(2), pp.138–147.

Budi, E. *et al*. (2021). Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di *Era Society* 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, *3*, pp.223–234.

Gunawan, F. *et al*. (2024). Membangun Benteng Digital Untuk Memperkuat Etika *Cyber Security* Melawan Ancaman *Cyber Crime*. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1), pp.154–167.

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. *Jurnal Ilmiah Manajemen Informatika dan Komputer*, *1*(2), pp.63–70.

Khotimah, H. *et al*. (2022). Implementasi *Security Information And Event Management* (SIEM) Pada Aplikasi SMS Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi*, *3*(2), pp.213–219.

Nasher, F. (2018). Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (LPSE) Di Dinas Komunikasi Dan

Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013. *Media Jurnal Informatika*, *10*(1), pp.1–16.

Nova, S. D. *et al*. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, *9*(13), pp.225–236.

Novianto, E. *et al*. (2023). Keamanan Informasi (*Information Security)* Pada Aplikasi Sistem Informasi Manajemen Kepegawaian Dengan *Defense In Depth*. *J-Icon: Jurnal Komputer dan Informatika*, *11*(1), pp.1–6.

Ramadhani, N. D. *et al*. (2020). Evaluasi Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kabupaten Malang Menggunakan Indeks KAMI (Keamanan Informasi). *Jurnal pengembangan teknologi informasi dan ilmu komputer*, *4*(5), pp.1490–1498.

Saputra, F. *et al*. (2024). Peneraan Manajeme *Security* Terhadap *Cyber Crime* Di Kominfo. *IJM: Indonesian Journal of Multidiciplinary*, *2*(1), pp.146–154.

Soesanto, E. *et al*. (2023). Peran Manajemen Sekuriti di Bank BRI Dalam Pengamanan File Nasabah untuk Mencegah Ancaman *Cyber Security* dan Menjaga Objektivitas Nasional. *IJM: Indonesian Journal of Multidiciplinary*, *1*(2), pp.497–502.

Sufi, F. Y. N. *et al*. (2023). Analisis Ancaman *Cybercrime* Dan Peran Sistem Biometrik*: Systematic Literature Review*. *Prosiding senapan : seminar nasional akuntansi*, *3*(1), pp.19–29.

Waruwu, M. (2024). Pendekatan Penelitian Kualitatif: Konsep, Prosedur, Kelebihan dan Peran di Bidang Pendidikan. *Afeksi: Jurnal Penelitian dan Evaluasi Pendidikan*, *2*(2).