Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 73-84
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Efektivitas Cyber Law dalam Menanggulangi Pelanggaran Cybersecurity

Desinta Widurizky [1], Elisabet Simatupang [1], Nadiyah Rahmadani [1], Syifa Rahma Auliasyah [1,*]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Bekasi Utara, (021)889558822; e-mail: 202310715296@mhs.ubharajaya.ac.id, 202310715044@mhs.ubharajaya.ac.id, 202310715131@mhs.ubharajaya.ac.id, 202310715088@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202310715088@mhs.ubharajaya.ac.id

Diterima: 17 Des 24; Review: 26 Des 24; Disetujui: 26 Des 24; Diterbitkan: 27 Des 24

Abstract

In the growing digital era, information security information security is very crucial. This research explores the effectiveness of Cyber Law implementation in overcoming cyber security violations at Bhayangkara University, Greater Jakarta. Bhayangkara University, Greater Jakarta. By using quantitative research method quantitative research method, data was collected through distributing questionnaires to 295 respondents from informatics study program students. This research identified challenges faced, including the public's low understanding of Cyber Law and the lack of socialization in the university environment. Analysis result analysis showed that while there is an increased awareness of the importance of Cyber Law, there are still shortcomings in the application of sanctions and the protection of personal data. personal data protection. The Waterfall method was used to design a structured security system, ensuring each stage of development is optimized. This research provides recommendations to improve the understanding and application of Cyber Law to strengthen cybersecurity among university students.
Keywords: *Cyber Law, cybersecurity, Waterfall method, data protection, quantitative research.*

Abstrak

Dalam era digital yang semakin berkembang, keamanan informasi menjadi hal yang sangat krusial. Penelitian ini mengeksplorasi efektivitas penerapan Cyber Law dalam mengatasi pelanggaran keamanan siber di Universitas Bhayangkara Jakarta Raya. Dengan menggunakan metode penelitian kuantitatif, data dikumpulkan melalui penyebaran kuisioner kepada 295 responden dari mahasiswa program studi informatika. Penelitian ini mengidentifikasi tantangan yang dihadapi, termasuk rendahnya pemahaman masyarakat tentang Cyber Law dan minimnya sosialisasi di lingkungan universitas. Hasil analisis menunjukkan bahwa meskipun ada peningkatan kesadaran tentang pentingnya Cyber Law, masih terdapat kekurangan dalam penerapan sanksi dan perlindungan data pribadi. Metode Waterfall digunakan untuk merancang sistem keamanan yang terstruktur, memastikan setiap tahap pengembangan dioptimalkan. Penelitian ini memberikan rekomendasi untuk meningkatkan pemahaman dan penerapan Cyber Law guna memperkuat keamanan siber di kalangan mahasiswa.

Kata kunci: Cyber Law, keamanan siber, metode Waterfall, perlindungan data, penelitian kuantitatif.

1. Pendahuluan

Dalam era digital saat ini, keamanan informasi menjadi salah satu aspek yang sangat krusial, mengingat teknologi informasi telah menjadi fondasi utama dalam berbagai aspek kehidupan masyarakat, termasuk sektor ekonomi, pendidikan, kesehatan, dan pemerintahan. Namun, kemajuan teknologi yang pesat juga membawa tantangan baru, yakni peningkatan ancaman terhadap keamanan informasi, khususnya dalam bentuk pelanggaran cybersecurity. Pelanggaran semacam ini dapat berdampak serius, baik secara individu, organisasi, maupun negara, sehingga memerlukan perhatian dan tindakan khusus untuk mitigasinya (Hoshmand et al., 2023). Peningkatan pelanggaran cyber terjadi karena semakin tingginya ketergantungan masyarakat pada teknologi digital, yang menyebabkan semakin banyaknya informasi pribadi dan keuangan yang disimpan secara digital. Hal ini menjadikan keamanan informasi sebagai tantangan utama di era modern, mengingat pelanggaran semacam ini tidak hanya menimbulkan kerugian finansial tetapi juga mengakibatkan kebocoran informasi sensitif. Pelanggaran cybersecurity dapat memberikan dampak yang luas, termasuk membahayakan individu, bisnis, hingga negara. Akibatnya, data dan informasi penting bisa rusak, hilang, atau dimanipulasi, sehingga keamanan informasi tidak dapat berjalan secara optimal. Untuk mengatasi dan meminimalisir pelanggaran semacam ini, dibutuhkan pendekatan yang tepat. Salah satu metode yang dianggap efektif adalah penerapan cyber law, yaitu regulasi hukum yang dirancang khusus untuk mengatur dan melindungi aktivitas di dunia maya. Cyber law adalah aspek hukum yang berasal dari istilah Cyberspace law, yang mencakup berbagai hal yang berkaitan dengan individu atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet serta elektronik. Cyber law mulai berlaku ketika seseorang atau entitas hukum mulai online dan terlibat dalam dunia cyber atau maya. (*Cyber Law*, 2024) (*Cyber Law: Apa Itu?*, 2021). *Cyber law* bertumpu pada disiplin ilmu hukum yang terdahulu antara lain: Hukum Kekayaan Intelektual (HKI), hukum perdata, hukum perdata internasional dan hukum internasional (Law et al., 2014). Cyber law memiliki ruang lingkup yang sangat luas, mencakup berbagai aspek hukum yang terkait dengan aktivitas di dunia maya. Salah satu fokus utamanya adalah perlindungan terhadap Hak Kekayaan Intelektual (HKI), yang meliputi hak cipta, hak paten, hak merek, rahasia dagang, dan desain industri. Kejahatan di bidang ini sering kali menjadi perhatian utama karena dampaknya yang signifikan terhadap pemilik hak dan perekonomian. Kejahatan itu adakalanya dengan *carding*, *hacking*, *cracking,* dan *cybersquanting*.

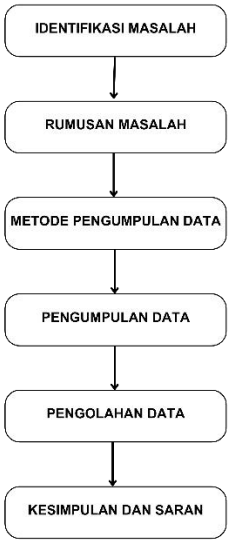
Dalam meminimalisir kejahatan-kejahatan tersebut, *cyber law* memiliki kelebihan yaitu perlindungan terhadap data pribadi dari penyalahgunaan, pencurian identitas, dan pelanggaran privasi, membuat regulasi terhadap tindakan kriminal dan menetapkan beberapa regulasi tersebut untuk platform di dunia maya, namun begitu *cyber law* juga mempunyai kekurangan seperti perubahan teknologi yang cepat, penerapan regulasi yang beragam. Sehingga dari kelebihan dan kelemahan tersebut perlu diadakannya penerapan efektifitas *cyber law* di tempat di mana *cyber law* itu akan diimplementasikan.

Efektifitas *cyber law* terbagi menjadi berberapa aspek, seperti kejelasan tentang regulasi *cyber law* yang ingin diterapkan, kesadaran tentang *cybersecurity* di lingkungan masyarakat, penegakan aparat hukum yang efektif di bidang *cyber*, penyesuaian terhadap perkembangan teknologi yang ada, sanksi yang tepat bagi para pelanggar, dan evaluasi regulasi yang diterapkan secara berkala. Aspek-aspek tersebut diharapkan dapat meningkatkan efektifitas *cyber law* untuk menanggulangi pelanggaran di bidang *cyber*.

Untuk mengetahui seberapa efektifnya penerapan *cyber law* untuk menanggulangi pelanggaran di bidang *cyber*. Peneliti akan melakukan penelitian di lingkungan Universitas Bhayangkara Jakarta Raya, Peneliti juga akan menyebarkan kuisioner dengan target responden yang peneliti harapkan berasal dari kalangan mahasiswa dan mahasiswi program studi informatika pada fakultas ilmu komputer semester tiga, lima, dan tujuh dengan target responden sebanyak 295 orang.

2. Metode Penelitian

2.1 Kerangka Penelitian



Sumber: Hasil Penelitian (2024)

Gambar 1. Kerangka Penelitian

Pada gambar 1 menunjukan penelitian ini dirancang secara sistematis untuk menjawab permasalahan terkait efektivitas *cyber law* dalam meminimalisir pelanggaran di bidang keamanan siber di lingkungan Universitas Bhayangkara Jakarta Raya. Permasalahan yang diidentifikasi mencakup tiga aspek utama, yaitu rendahnya tingkat pemahaman masyarakat mengenai *cyber law*, minimnya sosialisasi tentang *cyber law* di lingkungan universitas, dan kurangnya kesadaran akan pentingnya penerapan *cyber law* dalam mendukung keamanan siber. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menjawab rumusan

masalah: Bagaimana cara mengukur efektivitas *cyber law* dalam meminimalisir pelanggaran di bidang keamanan siber di lingkungan Universitas Bhayangkara Jakarta Raya.

Penelitian ini menggunakan dua metode utama dalam pengumpulan data, yaitu penyebaran kuisioner secara daring menggunakan *platform* Google Form untuk memperoleh data primer, serta studi literatur untuk mendukung analisis melalui sumber-sumber relevan. Data yang terkumpul dianalisis menggunakan perangkat lunak statistik SPSS melalui tahapan pengukuran data, pembuatan grafik untuk memvisualisasikan hasil secara informatif, dan analisis data untuk mendukung penarikan kesimpulan. Hasil penelitian ini memberikan gambaran mengenai efektivitas *cyber law* dalam konteks keamanan siber, serta menjadi dasar untuk memberikan rekomendasi guna meningkatkan pemahaman dan penerapan *cyber law* di masa depan.

2.2 *Cyberlaw*

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang dirancang untuk mengatur berbagai aktivitas yang terjadi di dunia digital. Ruang lingkup cyber law mencakup berbagai aspek yang berhubungan dengan individu atau subjek hukum yang memanfaatkan teknologi internet dan elektronik. Dalam praktiknya, cyber law mencakup aturan dan regulasi yang mengatur aktivitas di dunia maya, termasuk transaksi elektronik, perlindungan data, keamanan informasi, hak kekayaan intelektual, serta berbagai jenis kejahatan siber. Penerapan cyber law bertujuan untuk memberikan perlindungan hukum, menciptakan keadilan, dan menjaga keteraturan di ruang digital yang semakin kompleks (Fitri, 2022).

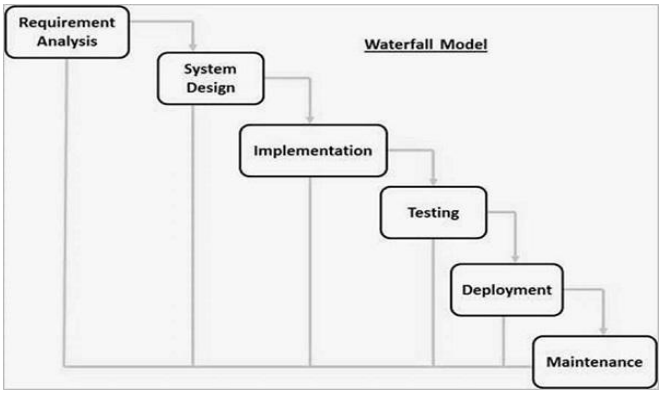
Cyber Law memiliki peran yang sangat penting dalam upaya pencegahan dan penanganan tindak pidana, khususnya yang dilakukan melalui sarana elektronik dan komputer. Cyber law memberikan dasar hukum yang kokoh bagi proses penegakan hukum terhadap berbagai kejahatan yang terjadi di dunia digital termasuk kejahatan pencucian uang dan kejahatan terorisme (Hasan dkk., 2024) (*Cyber Law: Pengertian Dan Tujuan Cyber Law Di Indonesia*, 2021).

2.3 *Waterfall*

Waterfall adalah salah satu model pengembangan perangkat lunak yang paling banyak digunakan, terutama dalam pendekatan tradisional. Model ini dikenal juga sebagai model klasik karena strukturnya yang sederhana dan terorganisir dengan baik. Dalam model Waterfall, proses pengembangan perangkat lunak dilakukan secara sekuensial dan teratur, di mana setiap tahap harus diselesaikan sepenuhnya sebelum tahap berikutnya dimulai (Anggraini dkk., 2023).

Metode Waterfall adalah salah satu metode yang sering digunakan dalam pengembangan perangkat lunak. Metode ini memiliki pendekatan yang sistematis dan terstruktur, di mana proses pengembangan perangkat lunak dilakukan secara bertahap, dengan setiap tahap bergantung pada penyelesaian tahap sebelumnya, seperti aliran air yang mengalir ke bawah dalam sebuah air terjun (Harjono & Kristianus Jago Tute, 2022)

Metode *waterfall* terdiri dari berberapa proses-proses. Adapun proses tersebut adalah sebagai berikut:



Sumber: (Syahrul & Priambodo, 2022)

Gambar 2. Tahapan proses waterfall

Pada gambar 2 menunjukan tahapan-tahapan proses *waterfall*. Mulai dari *requirement analyst*, *system design*, *implementation*, *testing*, *deployment*, dan *maintenance*.

3. Hasil dan Pembahasan

Pada bagian ini, peneliti akan membahas hasil penelitian ini, yaitu dimulai dari analisis terhadap kebutuhan penelitian hingga hasil olah data. Hasil penelitian tersebut akan dituliskan sesuai dengan alur kerja dari metode *waterfall*.

3.1. *Requirement Analysis*

Analisis dari kebutuhan pendukung untuk penelitian ini seperti pada tabel 1 berikut ini:

Tabel 1. Analisis Kebutuhan Penelitian

No.	Nama Alat atau *Tools*	Keterangan
1.	Laptop Acer Spin	Operasional penelitian
2.	Google Form	Data responden
3.	Microsoft Excel	Analisis data responden
4.	SPSS	Olah data responden
5.	Microsoft Word	Penulisan jurnal penelitian

Sumber: Hasil Penelitian (2024)

Pada tabel 1 menjelaskan bahwa terdapat lima alat atau tools yang dipergunakan peneliti untuk operasional penelitian ini. Dimulai dari laptop, Google Form, Microsoft Excel, SPSS, dan Microsoft Word.

3.2 *System Design*

Pada tahap ini, desain sistem difokuskan pada pengembangan rencana yang terstruktur untuk meningkatkan keamanan siber dan memastikan penerapan hukum siber secara efektif. Tahap desain meliputi pembuatan kerangka kerja yang mencakup arsitektur sistem, aliran data, antarmuka pengguna, dan titik integrasi, sesuai dengan prinsip-prinsip metode *Waterfall*.

Arsitektur Sistem

Arsitektur berlapis diusulkan, meliputi:

- Lapisan Presentasi: Antarmuka pengguna untuk administrator, ahli hukum, dan pengguna, yang memungkinkan akses dan navigasi yang aman (Fitri, 2022).
- Lapisan Logika Bisnis: Implementasi aturan dan protokol untuk keamanan siber, termasuk pemantauan, deteksi, dan pelaporan ancaman siber (Syahrul & Priambodo, 2022).
- Lapisan Data: Penyimpanan basis data yang aman untuk data pengguna, laporan, dan jejak audit, memastikan kepatuhan terhadap regulasi hukum siber (Fitri, 2022).

Desain Aliran Data

Data mengalir antar modul dengan aman, menggunakan teknik enkripsi untuk melindungi informasi selama transmisi, penyimpanan, dan akses (Syahrul & Priambodo, 2022).

Desain Antarmuka Pengguna

Fokus pada kemudahan penggunaan sambil memastikan keamanan yang kuat. Desain ini mencakup langkah-langkah kontrol akses dan proses otentikasi untuk membatasi penggunaan yang tidak sah (Fitri, 2022).

Titik Integrasi

Sistem akan terintegrasi dengan alat keamanan siber eksternal untuk deteksi dan respon terhadap ancaman. Juga akan terhubung dengan basis data untuk memvalidasi kepatuhan hukum (Syahrul & Priambodo, 2022).

3.3 *Implementation*

Desain sistem yang terstruktur ini menjadi dasar untuk menerapkan praktik terbaik keamanan siber menggunakan pendekatan *Waterfall*, memastikan setiap tahap dimulai dari analisis hingga pemeliharaan didokumentasikan secara menyeluruh dan sesuai dengan persyaratan hukum siber (Fitri, 2022), (Syahrul & Priambodo, 2022).

Pada tahap implementasi, sistem yang sudah dirancang akan dikembangkan sesuai dengan spesifikasi yang telah ditentukan. Proses ini melibatkan penerapan kode program, pengujian awal, dan penyesuaian terhadap kebutuhan spesifik untuk keamanan siber dan penerapan hukum siber. Tahap ini mengikuti alur metodologi Waterfall yang mencakup beberapa langkah penting:

1. Pengkodean Sistem: Pada tahap ini, pengkodean dilakukan berdasarkan desain sistem yang sudah dirancang sebelumnya. Penggunaan bahasa pemrograman yang tepat

dipilih sesuai dengan kebutuhan sistem keamanan siber yang mendukung enkripsi data dan otentikasi pengguna (Fitri, 2022).

2. Integrasi Modul: Setelah setiap modul selesai dikembangkan, modul-modul tersebut diintegrasikan untuk membentuk sistem yang utuh. Integrasi ini memastikan bahwa semua komponen bekerja secara sinergis sesuai dengan arsitektur yang telah direncanakan, termasuk integrasi alat-alat keamanan siber eksternal (Syahrul & Priambodo, 2022).
3. Pengujian Fungsional Awal: Pengujian fungsional dilakukan untuk memastikan setiap fitur berjalan sesuai dengan spesifikasi. Pada tahap ini, fokus utama adalah pada pengujian terhadap komponen keamanan, seperti sistem enkripsi data, kontrol akses, dan pencatatan jejak audit (Fitri, 2022), (Syahrul & Priambodo, 2022).
4. Penyesuaian dan Debugging: Hasil dari pengujian awal digunakan untuk melakukan debugging dan penyesuaian sistem agar sesuai dengan kebutuhan pengguna. Setiap modul diperbaiki jika ditemukan adanya bug atau kesalahan pada sistem keamanan siber (Anggraini dkk., 2023).

3.4 *Testing*

Pada tahap pengujian ini, data dari survei yang dikumpulkan digunakan untuk mengevaluasi efektivitas penerapan *Cyber Law* di lingkungan Universitas Bhayangkara Jakarta Raya. Uji coba ini dilakukan dengan mengacu pada hasil survei yang melibatkan 295 responden mahasiswa, mencakup beberapa aspek keamanan siber di kampus. Pengujian ini dilakukan melalui langkah-langkah sebagai berikut:

1. Analisis Data Survei

   Data yang dikumpulkan dari survei kalagan mahasiswa dan mahasiswi program studi informatika pada fakultas ilmu komputer semester tiga, lima, dan tujuh dengan target responden sebanyak 295 orang menunjukkan persepsi dan pengetahuan mahasiswa terhadap *Cyber Law* di kampus. Dari hasil survei, diperoleh data mengenai tingkat kesadaran dan pemahaman mahasiswa tentang aturan *Cyber Law*, frekuensi pelanggaran keamanan yang mereka dengar, serta efektivitas perlindungan yang dirasakan. Analisis data survei ini menjadi dasar untuk menguji apakah sistem yang diterapkan telah memenuhi tujuan yang ditetapkan dalam penelitian.
2. Validasi Terhadap Kejelasan Informasi *Cyber Law*

Seberapa jelas informasi tentang Cyber Law yang anda dapatkan dari kampus?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Jelas	15	5.1	5.1	5.1
	Jelas	128	43.4	43.4	48.5
	Tidak Terlalu Jelas	127	43.1	43.1	91.5
	Tidak Jelas Sama Sekali	25	8.5	8.5	100.0
	Total	295	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Gambar 3. Validasi Kejelasan Informasi *Cyber Law*

Pada gambar 3 menunjukan data survei, sebanyak 43.4% responden merasa bahwa informasi terkait *Cyber Law* cukup jelas, namun 43.1% merasa kurang jelas. Pengujian dengan menyebarkan kembali informasi *Cyber Law* melalui sistem keamanan baru yang dirancang, lalu mengevaluasi apakah terjadi peningkatan pemahaman di antara mahasiswa melalui kuesioner lanjutan. Validasi ini bertujuan untuk mengukur efektivitas sistem dalam meningkatkan kejelasan informasi.

3. Pengujian Keamanan *Wi-Fi* dan Sistem Internet Kampus

Apakah anda merasa aman saat menggunakan Wi-Fi atau fasilitas internet di kampus?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Aman	33	11.2	11.2	11.2
	Aman	156	52.9	52.9	64.1
	Kurang Aman	95	32.2	32.2	96.3
	Tidak Aman	11	3.7	3.7	100.0
	Total	295	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Gambar 4. Pengujian Keamanan *Wi-Fi* dan Sistem Internet Kampus

Pada gambar 4 menunjukan sebanyak 52.9% responden merasa aman menggunakan *Wi-Fi* kampus, tetapi 32.2% merasa kurang aman. Untuk menguji keamanan sistem yang baru, dilakukan simulasi serangan siber pada jaringan *Wi-Fi* kampus. Pengujian ini meliputi deteksi kerentanan sistem dan respons keamanan sistem dalam menghadapi ancaman yang diujikan. Hasil pengujian akan membandingkan tingkat keamanan sebelum dan sesudah penerapan sistem yang baru.

4. Evaluasi Efektivitas Penerapan Sanksi

Apakah menurut anda pihak kampus memberikan sanksi yang tegas kepada pelanggar Cyber Law?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Setuju	102	34.6	34.6	34.6
	Setuju	132	44.7	44.7	79.3
	Tidak Setuju	47	15.9	15.9	95.3
	Sangat Tidak Setuju	14	4.7	4.7	100.0
	Total	295	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Gambar 5. Evaluasi Efektivitas Penerapan Sanksi

Pada gambar 5 menunjukan data survei, hanya 34.6% responden sangat setuju bahwa kampus memberikan sanksi tegas terhadap pelanggaran, dan 44.7% setuju. Pengujian ini dilakukan dengan menilai apakah penerapan sistem keamanan siber yang baru

dapat memperkuat proses penegakan hukum di kampus. Fokusnya adalah pada kemudahan pelaporan pelanggaran dan apakah sistem baru dapat meningkatkan transparansi dalam pemberian sanksi bagi pelanggaran yang terjadi.

5. Pengujian Perlindungan Data Pribadi dan Sistem Akademik

Seberapa efektif Cyber Law dalam melindungi sistem akademik kampus seperti portal mahasiswa atau email kampus?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Efektif	38	12.9	12.9	12.9
	Efektif	164	55.6	55.6	68.5
	Kurang Efektif	85	28.8	28.8	97.3
	Tidak efektif Sama Sekali	8	2.7	2.7	100.0
	Total	295	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Gambar 6. Pengujian Perlindungan Data Pribadi dan Sistem Akademik

Pada gambar 6 menunjukan bahwa 55.6% responden merasa bahwa *Cyber Law* efektif dalam melindungi sistem akademik, namun 28.8% merasa kurang efektif. Pengujian ini dilakukan dengan menilai sejauh mana sistem keamanan siber yang baru mampu melindungi data pribadi mahasiswa, seperti informasi pada portal akademik dan email kampus. Pengujian ini melibatkan simulasi akses tidak sah dan pengujian respons sistem terhadap upaya pelanggaran.

6. Analisis Hasil Pengujian

Setelah seluruh pengujian selesai dilakukan, hasilnya dianalisis untuk menentukan apakah sistem baru yang diimplementasikan telah memenuhi kriteria yang diharapkan. Analisis ini mencakup perbandingan antara data survei awal dengan hasil survei setelah pengujian sistem dilakukan, untuk mengukur perubahan tingkat pemahaman, keamanan, dan efektivitas penerapan *Cyber Law* di kampus.

3.5 Deployment

Pada tahap *deployment*, sistem keamanan siber yang baru diterapkan di lingkungan Universitas Bhayangkara Jakarta Raya. Proses ini mencakup beberapa langkah penting untuk memastikan bahwa sistem dapat beroperasi secara efektif dalam kondisi nyata. Langkah-langkah yang dilakukan selama deployment meliputi:

1. Instalasi Sistem Keamanan

Instalasi mencakup implementasi perangkat lunak dan perangkat keras yang diperlukan untuk meningkatkan keamanan jaringan, termasuk sistem pemantauan dan enkripsi data. Sistem diintegrasikan dengan infrastruktur kampus yang ada, memastikan semua modul berjalan sesuai dengan spesifikasi (Syahrul & Priambodo, 2022).

2. Pelatihan Pengguna Akhir

   Pelatihan diberikan kepada pengguna akhir, termasuk mahasiswa, staf pengajar, dan administrator, untuk memastikan bahwa mereka memahami cara menggunakan sistem baru. Fokus pelatihan adalah pada proses otentikasi yang aman, cara melaporkan pelanggaran, serta langkah-langkah pencegahan dasar yang harus dilakukan (Fitri, 2022).
3. Pengujian Akhir Pasca-*Deployment*

   Setelah sistem diimplementasikan, dilakukan pengujian akhir untuk memastikan bahwa semua fungsi berjalan dengan baik di lingkungan nyata. Ini termasuk uji coba dengan beban nyata dan simulasi insiden keamanan untuk memvalidasi respons sistem (Anggraini dkk., 2023).
4. Sosialisasi Kebijakan Keamanan Siber

   Dilakukan sosialisasi mengenai kebijakan *Cyber Law* dan tata cara penggunaan sistem keamanan yang baru kepada seluruh warga kampus. Hal ini dilakukan untuk meningkatkan kesadaran terhadap pentingnya keamanan siber dan mengurangi pelanggaran di masa depan (Hasan dkk., 2024).

3.6 *Maintenance*

Pada tahap *Maintenance*, sistem keamanan siber yang baru secara rutin diperiksa dan diperbarui untuk menjaga kinerja dan keandalannya. Beberapa langkah dalam proses pemeliharaan ini meliputi:

1. *Monitoring* Sistem Secara Berkala

   Sistem dipantau secara rutin untuk mendeteksi potensi ancaman dan kerentanan baru yang mungkin muncul. *Monitoring* dilakukan menggunakan alat deteksi ancaman yang terintegrasi, serta pengawasan manual oleh tim keamanan siber kampus (Syahrul & Priambodo, 2022).
2. Pembaruan Perangkat Lunak Keamanan

   Pembaruan dilakukan secara berkala untuk memastikan bahwa sistem keamanan selalu menggunakan teknologi terbaru. Ini termasuk update untuk sistem enkripsi, *firewall*, serta perangkat lunak pemantauan yang ada pada sistem (Fitri, 2022).
3. Audit Keamanan dan Evaluasi Berkala

   Audit keamanan dilakukan setiap enam bulan untuk menilai efektivitas sistem dan memastikan bahwa semua kebijakan keamanan siber dipatuhi. Hasil audit digunakan untuk mengevaluasi sistem dan menentukan apakah ada penyesuaian atau perbaikan yang diperlukan (Anggraini dkk., 2023).
4. Dukungan Pengguna dan Layanan Teknis

   Tim teknis disediakan untuk menangani masalah yang dihadapi oleh pengguna terkait keamanan siber. Layanan dukungan ini mencakup bantuan teknis, pemulihan data, dan pelatihan tambahan jika diperlukan (Hasan dkk., 2024).

Tabel 2. Nilai Interval

Interval Skor	Kategori Persepsi	Persentase Responden (%)
0%-24,99%	Sangat (Tidak Setuju/Buruk/Kurang Sekali)	8.5%
25%-49,99%	(Tidak Setuju/Buruk/Kurang Sekali)	43.4%
50%-74,99%	(Setuju/Baik/Suka)	43.1%
75%-100%	Sangat (Setuju/Baik/Suka)	5.1%

Sumber: Hasil Penelitian (2024)

Tabel 2 menjelaskan kriteria yang dibutuhkan untuk evaluasi penerapan *Cyber Law* di kampus, berdasarkan hasil survei yang dilakukan kepada mahasiswa Universitas Bhayangkara Jakarta Raya. Adapun beberapa kriteria yang telah ditentukan, yaitu sebagai berikut: pada interval 0%-24,99%, responden yang memberikan nilai sangat rendah menilai bahwa penerapan *Cyber Law* sangat buruk atau tidak efektif. Pada interval 25%-49,99%, responden merasa penerapan *Cyber Law* kurang efektif, tetapi ada beberapa aspek yang dapat diterima. Sementara itu, pada interval 50%-74,99%, responden merasa bahwa penerapan *Cyber Law* cukup baik dan setuju bahwa kebijakan tersebut sudah cukup memadai. Terakhir, pada interval 75%-100%, responden yang sangat setuju dengan penerapan *Cyber Law* merasa bahwa kebijakan yang diterapkan sangat baik dan efektif dalam menjaga keamanan siber di kampus.

4. Kesimpulan

Hasil penelitian ini mengindikasikan bahwa penerapan *Cyber Law* di Universitas Bhayangkara Jakarta Raya telah memberikan kontribusi yang signifikan terhadap peningkatan keamanan siber. Penggunaan metode *Waterfall* dalam pengembangan sistem memastikan prosedur yang terstruktur dan sistematis. Tingkat kesadaran mahasiswa terhadap pentingnya *Cyber Law* mengalami peningkatan, meskipun masih diperlukan upaya lebih lanjut dalam hal pemahaman menyeluruh serta peningkatan keamanan jaringan. Perlindungan data dan sistem akademik menunjukkan perbaikan yang signifikan, namun efektivitas penerapan sanksi masih membutuhkan penguatan lebih lanjut.

Daftar Pustaka

Anggraini, Y., Fadillah, R., & Tuto Suban, N. (2023). Perancangan Sistem Informasi Persediaan Obat Pada Klinik Medika Prima Berbasis Web Menggunakan Metode Waterfall. *Teknik dan Multimedia*, *1*(2). http://www.php.net

Cyber law: Apa itu? (2021). Fahum Universitas Muhammadiyah Sumatera Utara. https://fahum.umsu.ac.id/cyber-law-apa-itu/

Cyber Law: Pengertian dan Tujuan Cyber Law di Indonesia. (2021). DSLA Law Firm. https://www.dslalawfirm.com/id/cyber-law

Cyber law. (2024). Telkom University. https://dte.telkomuniversity.ac.id/cyber-law/

Fitri, S. N. (2022). Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*, *7*(1), 104. https://doi.org/10.22373/justisia.v7i1.12719

Harjono, W., & Kristianus Jago Tute. (2022). Perancangan Sistem Informasi Perpustakaan Berbasis Web Menggunakkan Metode Waterfall. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, *2*(1), 47–51. https://doi.org/10.54259/satesi.v2i1.773

Hasan, Z., Alfath, M. R., Mahardika, A., Rizaldi, R., & Rizqullah, W. (2024). Peranan Cyber Law Dalam Penanganan Tindak Pidana Di Indonesia. *Jurnal Komunikasi*, *2*(5), 337–345.

Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains Dan Teknologi, 5(2), 679–686. https://doi.org/10.55338/saintek.v5i2.2347

Law, I., Tech, J. M. J. I., Privacy, L., & Kirchner, S. (2014). UIC John Marshall Journal of Information Technology & Privacy Beyond Privacy Rights : Crossborder Cyber-Espionage and BEYOND PRIVACY RIGHTS : CROSS- BORDER CYBER-ESPIONAGE AND. 31(3).

Syahrul, A., & Priambodo, J. (2022). Rancang Bangun Sistem Informasi Penjualan Sparepart Mobil Berbasis Web di Bengkel Maestro Auto Service Menggunakan Metode Waterfall. Dalam *Scientia Sacra: Jurnal Sains* (Vol. 2, Nomor 2). http://pijarpemikiran.com/index.php/Scientia