MAKALAH
ISU ETIKA, RISIKO, DAN PENANGANAN INSIDEN KEAMANAN DATA & SISTEM INFORMASI

Dosen Mata Kuliah : Riyang Gumelta, S.Kom., M.Kom

Disusun Oleh:

Amanda Nofitri	(2301161001)
Bintang Rhamadhan	(2301161002)
Dini Aprisia	(2301163001)

PROGRAM STUDI D3 SISTEM INFORMASI

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI PADANG

2025

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya makalah dengan judul Isu Etika, Risiko, Dan Penanganan Insiden Keamanan Data & Sistem Informasi ini dapat diselesaikan tepat waktu.

Makalah ini disusun untuk memenuhi tugas mata kuliah terkait etika profesi sekaligus menambah wawasan penulis mengenai isu-isu penting seputar etika, tren insiden, jenis serangan, karakteristik pelaku, penerapan pertahanan multilapisan, serta langkah penanggulangan serangan siber.

Penulis menyadari bahwa makalah ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun dari pembaca sangat diharapkan agar penulisan selanjutnya dapat lebih baik.

Akhir kata, penulis mengucapkan terima kasih kepada dosen mata kuliah, rekan-rekan mahasiswa, serta semua pihak yang telah membantu secara langsung maupun tidak langsung dalam penyusunan makalah ini.

Padang, 21 September 2025

Kelompok 3

DAFTAR ISI

BAB I
PENDAHULUAN

1. Latar Belakang

Keamanan data dan sistem informasi kini menjadi salah satu fondasi utama keberlangsungan organisasi, bisnis, dan pemerintahan. Setiap hari, miliaran transaksi dan pertukaran data terjadi secara daring. Perkembangan teknologi digital, *Internet of Things (IoT*), dan layanan berbasis cloud membuat data semakin mudah diakses dan dibagikan, tetapi sekaligus rentan terhadap penyalahgunaan.

Pertumbuhan eksponensial penggunaan data memperbesar potensi pelanggaran privasi, pencurian identitas, serta sabotase sistem kritis. Insiden besar mulai dari kebocoran basis data pelanggan hingga serangan ransomware pada infrastruktur vital membuktikan bahwa keamanan bukan lagi opsi, melainkan kebutuhan strategis. Tanpa pengamanan yang baik, kerugian finansial, reputasi, dan kepercayaan publik dapat terjadi dalam hitungan jam.

Di sisi lain, kompleksitas ancaman tidak hanya berasal dari faktor teknologi semata, tetapi juga manusia dan organisasi. Kesalahan pengguna, kelalaian prosedur, dan kurangnya kesadaran keamanan sering menjadi pintu masuk utama bagi penyerang. Oleh karena itu, strategi perlindungan data modern harus bersifat menyeluruh mencakup kontrol teknis, kebijakan organisasi, pelatihan pengguna, hingga rencana pemulihan insiden (*incident response plan*). Selain aspek teknis, ada persoalan etika: hak privasi individu, kewajiban organisasi menjaga kerahasiaan, serta transparansi penggunaan data. Isu-isu ini menjadikan keamanan data bukan hanya masalah teknologi, tetapi juga tanggung jawab sosial dan profesional.

2. Rumusan Masalah

a) Apa saja masalah etika yang berkaitan dengan pengamanan data dan sistem informasi?
b) Mengapa jumlah insiden keamanan komputer meningkat drastis dalam beberapa tahun terakhir?
c) Apa jenis serangan keamanan komputer yang paling umum terjadi?
d) Bagaimana karakteristik penjahat komputer dan frekuensi serangannya?
e) Apa elemen kunci dari proses multilapisan berdasarkan konsep jaminan (*assurance*)?
f) Tindakan apa saja yang tepat dilakukan dalam menanggapi insiden keamanan?

3. Tujuan Penulisan

a) Menjelaskan pentingnya keamanan data dan sistem informasi di era digital.
b) Menguraikan masalah etika yang timbul terkait pengamanan data.
c) Menganalisis faktor penyebab meningkatnya insiden keamanan.
d) Mengidentifikasi jenis serangan yang paling umum serta karakteristik pelaku.
e) Menjabarkan elemen kunci proses multilapisan berbasis konsep jaminan.
f) Memberikan gambaran langkah penanganan insiden keamanan.

4. Manfaat Penulisan

a) Bagi Mahasiswa/Peneliti: Menambah wawasan tentang keamanan siber, etika, dan praktik penanganan insiden.
b) Bagi Organisasi/Perusahaan: Memberi acuan dasar dalam menyusun kebijakan keamanan data dan prosedur respon insiden.

c) Bagi Masyarakat Umum: Meningkatkan kesadaran akan pentingnya melindungi informasi pribadi dan mengenali ancaman digital.
d) Bagi Pemerintah/Pembuat Kebijakan: Memberi masukan untuk memperkuat regulasi dan program literasi keamanan informasi

BAB II
LANDASAN TEORI

2.1 Definisi dan Konsep Dasar

2.1.1 Sistem Informasi

Menurut Laudon & Laudon (2022), “Sistem informasi adalah seperangkat komponen yang saling berhubungan untuk mengumpulkan, memproses, menyimpan, dan menyebarkan informasi guna mendukung pengambilan keputusan, koordinasi, dan kontrol dalam organisasi.”

2.1.2 Keamanan Sistem Informasi

Whitman & Mattord (2022) menyatakan bahwa keamanan informasi adalah perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi dari ancaman yang disengaja maupun tidak disengaja.

2.2 Etika dalam Teknologi Informasi

Stair & Reynolds (2021) berpendapat bahwa etika TI mencakup prinsip moral yang mengatur perilaku terkait pemrosesan, distribusi, dan penggunaan informasi. Mereka menekankan privasi, akurasi, properti, dan akses sebagai empat isu etika utama.

Prinsip penting tambahan:

a) Privasi: Hak individu mengontrol data pribadi.
b) Kerahasiaan: Kewajiban organisasi menjaga informasi sensitif.
c) Transparansi & Persetujuan: Organisasi wajib menjelaskan tujuan pengumpulan data dan memperoleh izin jelas.
d) Tanggung Jawab Profesional: Praktisi TI harus jujur, menghindari konflik kepentingan, dan melaporkan pelanggaran.

2.3 Peningkatan Insiden Keamanan

Andress (2023) menyoroti pertumbuhan pesat serangan siber yang didorong oleh transformasi digital, meningkatnya nilai data, dan ketersediaan alat serangan yang murah. Faktor-faktor utama yang memicu peningkatan insiden keamanan meliputi:

a) Faktor Teknologi: Perkembangan *IoT*, layanan komputasi awan (*cloud*), dan kecerdasan buatan (*AI*) memperluas permukaan serangan sehingga memunculkan lebih banyak celah keamanan.
b) Faktor Manusia: Kesalahan pengguna dan rekayasa sosial (*phishing*) masih menjadi pintu masuk utama bagi pelaku serangan.
c) Faktor Ekonomi: Monetisasi kejahatan siber, seperti ransomware, semakin mudah dan menguntungkan sehingga memotivasi pelaku.
d) Faktor Global: Perubahan pola kerja jarak jauh akibat pandemi *COVID-19* membuat jaringan rumah lebih rentan dibanding jaringan kantor yang terproteksi.

2.4 Jenis Serangan Umum

Menurut Singh et al. (2023), phishing, ransomware, dan serangan Distributed *Denial-of-Service* (*DDoS*) tetap menjadi ancaman dominan terhadap keamanan informasi dengan tren peningkatan pasca-pandemi.

Secara umum, jenis-jenis serangan yang sering terjadi meliputi:

a) *Phishing* dan Rekayasa Sosial: Upaya memanipulasi pengguna agar membocorkan kredensial atau informasi sensitif melalui email, pesan instan, atau media sosial.
b) *Malware*: Perangkat lunak berbahaya seperti virus, worm, ransomware, dan spyware yang dirancang untuk merusak sistem, mencuri data, atau mengenkripsi file korban.

c) *Denial-of-Service (DoS/DDoS*): Serangan yang membanjiri server atau jaringan sehingga layanan tidak dapat diakses oleh pengguna sah.
d) *Brute Force & Credential Stuffing*: Teknik menebak sandi secara sistematis atau menggunakan kredensial hasil kebocoran untuk memperoleh akses ilegal.
e) *Zero-Day Exploit*: Pemanfaatan kerentanan yang belum diketahui atau belum diperbaiki oleh pengembang sistem.
f) *Insider Threats*: Ancaman yang berasal dari orang dalam organisasi yang menyalahgunakan akses atau pengetahuannya terhadap sistem.

Beragam serangan ini menunjukkan bahwa ancaman terhadap sistem informasi bersifat berlapis dan terus berevolusi, sehingga organisasi perlu menerapkan strategi keamanan yang komprehensif.

2.5 Karakteristik Penjahat Komputer

Taylor et al. (2022) mengklasifikasikan penjahat komputer ke dalam beberapa kategori utama berdasarkan tingkat kemampuan, motivasi, dan keterlibatan mereka dalam aktivitas kejahatan siber.

Secara umum, tipe pelaku yang sering ditemui antara lain:

a) *Script Kiddies*: Pemula yang menggunakan alat jadi atau skrip buatan orang lain untuk melakukan serangan tanpa pemahaman mendalam.
b) *Cybercriminal Gangs*: Kelompok profesional yang bermotif finansial, mengorganisasi serangan secara sistematis untuk memperoleh keuntungan.
c) *Hacktivists*: Individu atau kelompok yang bermotif politik atau ideologi, menggunakan serangan untuk menyampaikan pesan atau protes.

d) *Nation-State Actors*: Agen negara yang melakukan spionase, sabotase, atau operasi siber untuk kepentingan strategis.

Motivasi di balik serangan ini beragam, mulai dari keuntungan finansial, ego pribadi, politik, balas dendam, hingga spionase. Laporan keamanan global menunjukkan bahwa rata-rata ribuan serangan terdeteksi setiap hari secara global, dengan sektor keuangan dan kesehatan menjadi target paling sering karena nilai datanya yang tinggi dan infrastruktur kritis yang dimilikinya.

2.6 Konsep Jaminan & Multilapisan

NIST SP 800-160 Rev. 1 (2021) menegaskan bahwa *defense in depth* atau pertahanan berlapis merupakan pendekatan keamanan yang melibatkan kombinasi kontrol teknis, kebijakan, kesadaran manusia, serta rencana pemulihan untuk mencapai tingkat jaminan keamanan yang dapat diverifikasi. Pendekatan ini tidak hanya mengandalkan satu mekanisme, tetapi menyusun beberapa lapisan pertahanan agar jika satu lapisan ditembus, lapisan berikutnya tetap memberikan perlindungan.

Secara umum, lapisan-lapisan yang dimaksud meliputi:

a) Lapisan Teknis: Implementasi *firewall*, sistem deteksi dan pencegahan intrusi (IDS/IPS), enkripsi, dan segmentasi jaringan untuk meminimalkan akses tidak sah.
b) Lapisan Kebijakan: Tata kelola keamanan, prosedur standar, dan manajemen risiko yang mengatur cara organisasi melindungi aset informasinya.
c) Pelatihan Pengguna: Edukasi anti *phishing*, pembiasaan penggunaan sandi yang kuat, serta peningkatan kesadaran keamanan bagi seluruh staf.

d) Monitoring & Audit: Penerapan logging, sistem SIEM, dan penilaian kerentanan secara rutin untuk mendeteksi potensi ancaman sejak dini.
e) Backup & Pemulihan: Penyusunan rencana pemulihan bencana *(Disaster Recovery Plan*) dan *business continuity* untuk memastikan layanan tetap berjalan setelah insiden.
f) Uji Keamanan: Pelaksanaan *penetration testing* dan latihan red team/blue team untuk mengevaluasi efektivitas pengendalian keamanan yang ada.

Pendekatan multilapisan ini memungkinkan organisasi mengurangi risiko secara signifikan karena setiap lapisan saling melengkapi dan memperkuat perlindungan terhadap ancaman yang terus berkembang.

2.7 Penanganan Insiden Keamanan

Penanganan insiden keamanan informasi merupakan proses sistematis untuk mengidentifikasi, merespons, dan memulihkan sistem dari gangguan atau serangan siber. NIST Computer Security Incident Handling Guide (SP 800-61 Rev. 1, 2021) menekankan pentingnya pendekatan terstruktur agar dampak serangan dapat diminimalkan dan layanan cepat pulih.

Secara umum, tahapan penanganan insiden mencakup:

a) Deteksi: Mengidentifikasi aktivitas abnormal melalui mekanisme monitoring, logging, dan peringatan dini.
b) Kontainmen: Mengisolasi sistem atau jaringan yang terdampak untuk mencegah penyebaran serangan ke bagian lain.
c) Eradikasi: Menghapus malware, memblokir akses yang tidak sah, serta memperbaiki kerentanan yang dimanfaatkan penyerang.

d) Pemulihan: Mengembalikan layanan dan memverifikasi integritas data serta sistem agar kembali normal.
e) Pelaporan & Komunikasi: Memberi tahu pemangku kepentingan internal dan, bila perlu, pihak berwenang sesuai regulasi yang berlaku.
f) Evaluasi Pasca-Insiden: Menganalisis akar penyebab insiden, mengevaluasi efektivitas respons, serta memperbarui kebijakan dan prosedur keamanan untuk pencegahan ke depan.

Pendekatan ini memastikan organisasi tidak hanya menanggapi insiden secara reaktif, tetapi juga belajar dari setiap kejadian untuk memperkuat sistem keamanan di masa mendatang.

BAB III
PEMBAHASAN

3.1 Analisis Masalah Etika

Kasus : 23andMe Data Breach (2023-2025)

3.1.1 Kronoligi

Pada tahun 2023, perusahaan layanan tes DNA asal Amerika Serikat, 23andMe, mengalami salah satu kebocoran data genetika terbesar dalam sejarah. Peretas memanfaatkan teknik credential stuffing menggunakan kembali kombinasi email dan kata sandi yang sebelumnya bocor dari situs lain, untuk masuk ke ribuan akun pelanggan. Akibatnya, data pribadi lebih dari 6,9 juta pengguna terekspos, termasuk informasi genetika dan silsilah keluarga yang sangat sensitif.

3.1.2 Masalah Etika Yang Muncul

Beberapa masalah etika yang muncul, antara lain:

a) Privasi Individu: Pengguna tidak hanya kehilangan data dasar (nama, alamat), tapi data genetika dan silsilah keluarga sangat sensitif. Apakah persetujuan awal mencakup kemungkinan penyalahgunaan data tersebut?
b) Transparansi & Kewajiban Pencatatan: Apakah 23andMe segera memberitahu pengguna setelah pelanggaran atau hanya setelah data muncul di publik? Kecepatan dan kejelasan pemberitahuan sering jadi masalah etika.
c) Keamanan & Tanggung Jawab Perusahaan: Apakah sistem autentikasi & kontrol akses memadai? Apakah mereka sudah menggunakan MFA (*multi factor authentication*)? Apakah ada langkah untuk memonitor penggunaan kembali password?

3.1.3 Penyelesaian

Berikut Jalan Penyesesaian nya :

a) 23andMe memaksa reset password pengguna.
b) Mengimplementasikan verifikasi dua langkah (*two-step verification*).
c) Memberi nasihat kepada pengguna untuk mengubah password di platform lainnya jika menggunakan password yang sama.

3.2 Analisis Tren Peningkatan Insiden

a) Organisasi mengalami rata-rata 1.876 serangan mingguan di Q3 2024, naik ~75% dibanding periode yang sama di 2023.
b) 88% CIO melaporkan bahwa organisasi mereka menghadapi insiden keamanan dalam 12 bulan terakhir.
c) *Ransomware & malware* jadi ancaman besar: ~72.7% organisasi kena serangan ransomware di 2023.
d) Rata-rata waktu untuk mendeteksi & mengendalikan pelanggaran data: 258 hari.
e) Biaya rerata per insiden pelanggaran data meningkat — sekitar US$4.88 juta per breach di 2024.

3.3 Analisis Jenis Serangan & Dampaknya

3.3.1 Jenis Serangan Umum

credential stuffing / reuse credentials, *ransomware*, *phishing*, *insider threat,* serangan terhadap sistem *cloud*. (dari kasus 23andMe & data statistik)

3.3.2 Dampak

Akibat :

a) Finansial: biaya langsung seperti pemulihan, kompensasi, denda regulasi; biaya tidak langsung seperti hilangnya pelanggan. Mis: biaya rata-rata US$4.88 juta per *breach*.

b) Reputasi dan Kepercayaan: pengguna kehilangan kepercayaan, bisa berdampak jangka panjang.
c) Operasional: *downtime*, gangguan layanan. Contohnya: Insiden Change Healthcare (2024) berdampak pada infrastruktur kesehatan besar, menunda pembayaran dan fasilitas medis.

3.4 Karakteristik Pelaku & Motif

3.4.1 Motif

finansial (*ransomware*, pencurian data & dijual), reputasi / ego, ideologi (*hacktivism*), spionase (aktor negara). Contoh: kelompok "ShinyHunters" yang membobol data pelanggan Kering/Gucci.

3.4.2 Karakter Pelaku

Antara Lain:

a) Profesional / kriminal terorganisir yang menggunakan alat canggih dan sumber daya.
b) Pelaku yang memanfaatkan kesalahan manusia (misalnya reuse password, kurangnya MFA). Kasus 23andMe sangat menonjol di sini.
c) Insider / human error: seperti kasus Lloyds yang salah mengirim dokumen pelanggan lain karena kesalahan manusia.

3.4.3 Frekuensi

Hampir semua organisasi besar/kecil pernah mengalami insiden dalam setahun terakhir (88% CIO melapor). Dan *Phishing* & penggunaan kembali kredensial muncul sangat sering.

3.5 Evaluasi Penerapan Proses Multilapisan di Organisasi Nyata

3.5.1 Kasus 23andMe

Tindakan Yang Diambil

a) Sebelum breach: sistem autentikasi standar, tapi kurang MFA, reuse password digunakan oleh pengguna.
b) Setelah breach: menerapkan reset password, MFA/verifikasi dua langkah untuk mengurangi reuse credentials.
c) Evaluasi: langkah-langkah ini membantu tapi remedial; idealnya sudah diterapkan sebelumnya.

3.5.2 Pembelajaran / kekurangan yang muncul:

Diantara lain :

a) Banyak organisasi terlambat mendeteksi pelanggaran (rata-rata butuh ratusan hari).
b) Kadang kontrol teknis ada, tapi pengguna kurang dilibatkan (kurang pelatihan), atau proses governance kurang kuat.
c) Keterbatasan respon cepat & komunikasi publik / regulator.

3.6 Rekomendasi Tindakan Penanggulangan

Berdasarkan studi kasus & data:

a) Perkuat autentikasi, wajibkan penggunaan MFA, password unik, deteksi *reuse credentials*.
b) Pelatihan keamanan & kesadaran pengguna, *phishing awareness* secara berkala, simulasi, edukasi penggunaan perangkat & password.
c) Implementasi *defense-in-depth*:
    - Firewall, segmentasi jaringan, enkripsi data dalam transit dan saat disimpan.
    - Sistem deteksi & respons insiden (IDS/IPS, SIEM).
    - Backup & pemulihan bencana (*disaster recovery plan*).

d) Audit & monitoring regular: audit internal & eksternal, penilaian kerentanan (*vulnerability assessment)*, *penetration testing.*
e) Transparansi & pemberitahuan cepat ketika terjadi pelanggaran, segera beri tahu pihak terdampak & otoritas regulasi sesuai aturan lokal.
f) Kebijakan keamanan & tata kelola yang kuat *governance* yang jelas, kepemilikan keamanan, pengelolaan risiko secara proaktif, kebijakan keamanan untuk pihak ketiga/vendor.
g) Peningkatan investasi & alokasi sumber daya baik SDM, anggaran teknologi keamanan, dan infrastrukturnya.

BAB IV
KESIMPULAN DAN SARAN

4.1 Kesimpulan

Penulis berkesimpulan bahwa keamanan data dan sistem informasi sangat penting di era digital karena perkembangan teknologi telah meningkatkan pemanfaatan data sekaligus risiko serangan siber. Kasus nyata seperti kebocoran data 23andMe membuktikan bahwa ancaman dapat menimpa organisasi besar. Masalah etika, seperti keterlambatan pemberitahuan kebocoran data, memperlihatkan perlunya tanggung jawab moral yang lebih kuat. Jenis serangan umum *phishing*, *ransomware*, dan *credential stuffing* menimbulkan dampak finansial, reputasi, dan operasional yang serius. Evaluasi pertahanan multilapisan menunjukkan bahwa penggunaan *autentikasi multi-faktor*, enkripsi, segmentasi jaringan, dan pelatihan karyawan efektif jika diterapkan konsisten.

4.2 Saran

Penulis menyarankan organisasi menerapkan pertahanan berlapis secara menyeluruh, memperkuat kebijakan keamanan, dan melatih kesadaran karyawan. Rencana tanggap insiden harus jelas dan transparansi kepada publik perlu dijaga untuk mempertahankan kepercayaan. Investasi pada teknologi deteksi dini dan kerja sama lintas sektor juga penting guna meminimalkan dampak serangan di masa depan.

DAFTAR PUSTAKA

Harjinder, S. L., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49.

Silvestri, S., Islam, S., Amelin, D., et al. (2024). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security*.

Rana, P., & Patil, B. P. (2023). Cyber security threats in IoT: A review. *Journal of Health and Safety*, *12*(4), 312–329.

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The new frontier of cybersecurity: Emerging threats and innovations. *arXiv preprint*.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *NIST Special Publication 800-160 Volume 2 Revision 1: Developing Cyber-Resilient Systems – A Systems Security Engineering Approach*. National Institute of Standards and Technology.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Taylor, R. E., Fritsch, E. J., & Liederbach, J. (2019). *Digital Crime and Digital Terrorism* (3rd ed.). Pearson.