Jurnal Kajian Stratejik Ketahanan Nasional

Volume 2
Number 2 *JKSKN Volume 2 No 2 2019*

Article 4

7-1-2019

Analisis Ancaman Terhadap Penerapan Framework Manajemen Insiden Di Indonesia

Rizky Hendra Kurniawan
Universitas Indonesia, xrhendra@gmail.com

Abdul Rivai Ras
Universitas Indonesia, rivai_ras@yahoo.com

Recommended Citation

Kurniawan, Rizky Hendra and Ras, Abdul Rivai (2019) "Analisis Ancaman Terhadap Penerapan Framework Manajemen Insiden Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*: Vol. 2: No. 2, Article 4.
DOI: 10.7454/jkskn.v2i2.10025
Available at: https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.2, 2019

Analisis Ancaman Terhadap Penerapan *Framework* Manajemen Insiden Di Indonesia

Rizky Hendra Kurniawan[1], Abdul Rivai Ras[2]

xrhendra@gmail.com; rivai_ras@yahoo.com

Abstract

The incident management framework is a tools that can be used as an early warning system to overcome problems in the implementation of information technology. This Framework also used for measuring the maturity level of incident management that has been carried out by institutions in Indonesia. We can used it as an open intelligence of information source. Within national scope, this framework used for knowing Indonesia's ability to deal with cyber incidents. Therefore, it is necessary to conduct a threat analysis on the implementation of incident management framework. Author used mix-methode research, which is the combination between qualitative and quantitative research. The result of this research is coefficient value of threat analysis to the implementation of incident management is 15.86. This value is included in high category.

Keywords: *Incident management, threat analysis, framework*

[1] Alumni Mahasiswa Kajian Ketahanan Nasional SKSG Universitas Indonesia
[2] Dosen Kajian Ketahanan Nasional SKSG Universitas Indonesia

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

1. Pendahuluan

Tantangan dan ancaman siber tidak dapat terhindarkan. Hal ini disebabkan oleh semakin pesatnya perkembangan dan penggunaan teknologi informasi di kalangan masyarakat Indonesia. Bahkan perkembangan teknologi ini dimanfaatkan oleh penyerang dalam melakukan berbagai serangan/ancaman terhadap layanan dan operasionalisasi di sektor Pemerintah, infrastruktur nasional, maupun ekonomi digital. Serangan/ancaman ini dapat berupa peretasan sistem, membangun opini di media sosial, penyebaran berita hoax, propaganda intelijen, melemahkan layanan yang dimiliki, dan kejahatan siber. Bahkan ancaman terhadap kejahatan siber ini telah dilakukan baik oleh aktor Negara maupun aktor non-negara, yang berdampak terhadap terjadinya cyber warfare atau cyber violence (Rahmawati, 2017).

Aspek rencana keberlangsungan layanan atau kegiatan terhadap adanya AGHT merupakan hal utama yang perlu direncanakan oleh pemilik layanan, sehingga dampak dari insiden siber yang terjadi dapat diminimalisir. Pengelolaan terhadap risiko dan dampak yang ditimbulkan sudah menjadi amanat yang harus dilaksanakan oleh seluruh Penyelenggara Sistem Elektronik (PSE) berdasarkan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Elektronik. Sejalan dengan hal tersebut, dikeluarkanlah Peraturan Presiden Nomor 18 tahun 2020 Tentang Rencana Pembangunan Jangka Menengah Nasional (RPJMN) Tahun 2020-2024. Pada Peraturan Presiden tersebut dijelaskan bahwa stabilitas Keamanan Nasional merupakan salah satu arah kebijakan yang diambil oleh Pemerintah dalam Pembangunan di bidang Politik, Hukum, Pertahanan dan Keamanan. Dalam menjaga stabilitas Keamanan Nasional tersebut, ancaman siber merupakan salah satu poin yang mendukung terselenggaranya dan terjaganya stabilitas keamanan nasional di ranah siber.

Kegagalan *early warning system* yang dibangun dalam mendeteksi adanya insiden siber berpotensi menyebabkan terjadinya krisis siber, sehingga dampak yang ditimbulkan cukup massif. Menurut hasil studi yang dilakukan oleh Frost & Sullivan tahun 2018, potensi kerugian ekonomi yang dialami oleh Indonesia akibat insiden keamanan siber mencapai USD 34,2 miliar atau sekitar Rp. 482,92 triliun (setara dengan 3,7% total PDB Indonesia). Studi tersebut juga menunjukkan bahwa 22% dari seluruh organisasi skala menengah dan skala besar di Indonesia pernah mengalami insiden siber. 27% organisasi yang disurvey tidak yakin telah mengalami insiden siber dikarenakan belum dilakukan investigasi terkait adanya potensi pembobolan data. Selain itu, kurangnya pengetahuan tentang counter intelligence dalam penanganan cyber attack juga menjadi salah satu titik lemah dalam menerapkan manajemen insiden pada institusi/perusahaan.

Oleh karena itu, penulis melakukan penelitian terkait analisis ancaman terhadap penerapan manajemen insiden dalam upayanya mendukung ketahanan nasional Indonesia. Adapun tujuan dari penelitian ini adalah mengukur potensi ancaman terhadap penerapan framework manajemen insiden di Indonesia. Selain itu, penelitian ini dapat pula digunakan sebagai bahan pertimbangan dalam menerapkan strategi penerapan manajemen insiden di Indonesia.

2. Metode Penelitian

Penulis menggunakan pendekatan penelitian mix-method. Pendekatan mix-method merupakan pendekatan penelitian yang mengkombinasikan jenis penelitian kualitatif dan kuantitatif. Metode ini akan sangat bermanfaat apabila dalam sebuah penelitian penggunaan metode kualitatif dan metode kuantitatif tidak cukup akurat dalam menentukan hasil penelitian apabila dilakukan secara sendiri-sendiri (Sugiyono, 2013). Metode kualitatif dilakukan dengan melakukan wawancara terhadap narasumber yang berasal dari para praktisi dan regulator di bidang keamanan siber. Hal ini bertujuan untuk

https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4
DOI: 10.7454/jkskn.v2i2.10025

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

mendapatkan gambaran yang lebih luas terkait dengan elemen-elemen yang nantinya digunaakan dalam melakukan analisis ancaman. Sedangkan metode kuantitatif digunakan dengan melakukan survey kepada 32 responden guna menilai indeks ancaman berdasarkan elemen ancaman yang telah dibuat sebelumnya. Adapun responden yang terlibat berasal dari para praktisi, regulator, dan private sector.

Metode ini juga diaplikasikan ketika peneliti memiliki pertanyaan yang perlu diuji dari segi outcome dan prosesnya, serta menyangkut kombinasi antara metode kuantitatif dan kualitatif dalam sebuah penelitian. Dengan digunakannya metode penelitian mix-method diharapkan dapat diperoleh data yang lebih komprehensif, reliabel, valid, dan objektif. Menurut Cresswell & Clark (2007), mix-method ini berfokus pada pengumpulan, analisis, dan pencampuran antara data kualitatif dan kuantitatif yang dilakukan dalam sebuah penelitian. Adapun skema penggabungan data yang digunakan dalam penelitian ini adalah baik data kualitatif dan data kuantitatif mendukung secara proporsional terhadap hasil penelitian yang dilakukan. Pendekatan ini dipilih oleh peneliti dikarenakan dalam penelitian yang dilakukan terdapat prosedur kuantifikasi yang digunakan dalam menilai potensi ancaman terhadap penerapan manajemen insiden di Indonesia.

Data yang akan dianalisis dalam tulisan ini adalah merupakan data primer yang didapatkan dari dua sumber data, yakni wawancara dan hasil survey kuesioner. Data primer pertama merupakan data yang didapatkan dari hasil wawancara kepada narasumber (sumber informasi) yang dianggap mampu dan mengetahui tentang topik yang dibahas dalam penelitian ini. Sedangkan data primer kedua merupakan data kuesioner responden yang digunakan dalam melakukan penghitungan terhadap analsis ancaman. Dalam penelitian ini, metode survey kuesioner dilakukan secara online. Adapun narasumber dan responden yang terlibat dalam penelitian ini terdiri dari regulator dan praktisi di bidang keamanan siber dan manajemen insiden. Adapun variabel yang digunakan dalam kuesioner ini terdiri dari 4 (empat) elemen ancaman, yakni keinginan, harapan, pengetahuan dan sumber daya.

Pemilihan narasumber dan responden ini didasarkan pada kompetensi dan pengalaman yang dimiliki, serta sesuai dengan tugas pokok dan fungsi yang diemban saat ini berkaitan dengan fokus penelitian yang diteliti. Narasumber dimaksud terbagi menjadi dua kategori yakni regulator dan praktisi. Regulator dapat diartikan sebagai pihak yang berwenang dalam kebijakan/aturan terkait dengan proses manajemen insiden. Sedangkan praktisi merupakan orang yang kesehariannya berkecimpung dalam ranah teknis manajemen insiden, dan secara tugas pokok merupakan pihak yang memahami baik secara teknis maupun non teknis terkait manajemen insiden. Responden dalam penelitian ini dipilih berdasarkan ruang lingkup tugas pokok yang bersangkutan dan kompetensi mereka dalam bidang keamanan siber.

Dalam tulisan ini, peneliti menggunakan triangulasi data sebagai metode untuk melakukan pemeriksaan terhadap keabsahan atau validitas data. Triangulasi data adalah mengumpulkan data dengan menggunakan beragam sumber data yang berbeda. Triangulasi data bertujuan untuk memastikan validitas data yang telah diperoleh dengan melakukan pengecekan dengan sumber lain (Apri, 2018). Proses triangulasi data dilakukan dengan membandingkan hasil wawancara antar narasumber yang memiliki latar belakang yang berbeda-beda, namun memiliki ruang lingkup tugas yang sama yakni di bidang manajemen insiden. Data yang didapatkan dari hasil wawancara diharapkan dapat saling melengkapi dan mengevaluasi jika terjadi bias dari setiap narasumber dengan latar belakang yang berbeda-beda.

3. Pembahasan

3.1.Teori Ancaman

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

Ancaman merupakan tujuan seseorang untuk membahayakan orang lain (Prunckun, 2019). Ancaman dapat dilakukan terhadap beberapa entitas seperti perorangan, organisasi, bahkan Negara. Dalam konteks penelitian ini, maka analisis ancaman yang dilakukan lebih diarahkan kepada ancaman terhadap penerapan manajemen insiden dalam konteks Negara.

Menurut Prunckun (2019), terdapat dua elemen utama yang digunakan dalam melakukan analisis ancaman, yakni threat intent dan threat capability. Threat intent merupakan optimisme dari pihak agen ancaman berkaitan dengan tingkat kesuksesan ketika melakukan serangan. Terdapat 2 (dua) elemen dalam threat intent, yakni elemen desire (keinginan) dan expectation (harapan). Keinginan dapat diartikan sebagai antusiasme dari pelaku serangan untuk menyebabkan terjadinya kerusakan/kegagalan. Sedangkan harapan merupakan keyakinan yang dimiliki pelaku bahwa tujuan yang diinginkan dapat tercapai jika rencananya terlaksana.

Threat capability merupakan kapabilitas dari agen ancaman dalam melakukan serangan terhadap target. Terdapat 2 (dua) elemen dalam threat capability, yakni elemen knowledge (pengetahuan) dan resource (sumberdaya). Pengetahuan diartikan sebagai informasi yang dimiliki oleh pelaku yang dapat mereka gunakan untuk mencapai tujuan yang diinginkan. Sedangkan sumber daya dapat diartikan sebagai kemampuan/pengalaman dan perlengkapan yang diperlukan untuk mewujudkan rencana pelaku.

3.2.Manajemen Insiden

Insiden Siber dapat pula diartikan sebagai satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik bagi layanan publik dan/atau pelanggaran kepatuhan terhadap kebijakan Keamanan Siber internal yang berlaku pada Penyelenggara Sistem Elektronik (PSE). Menurut ISO/IECTR18044:2004, insiden siber adalah satu/serangkaian peristiwa yang tidak diinginkan dan kemungkinan besar mengganggu proses bisnis dan mengancam keamanan informasi. Insiden adalah sebuah interupsi atau pengurangan kualitas dari layanan teknologi informasi (Silitonga & Ali, 2010).

Menurut ISO 27035 (2011), dijelaskan bahwa manajemen insiden merupakan serangkaian proses yang terdiri dari 5 (lima) fase, antara lain perencanaan dan persiapan, pendeteksian dan pelaporan, penilaian dan pengambilan keputusan, respon, dan pembelajaran. 5 (lima) fase ini merupakan langkah yang diambil dalam meminimalisir dampak negatif dari terjadinya insiden keamanan siber. Manajemen insiden juga merupakan proses yang dilakukan untuk menyelesaikan suatu insiden (Silitonga & Ali, 2010). Proses ini dilakukan berdasarkan masukan dari pengguna, laporan tim teknis, dan deteksi otomatis dari tools manajemen yang digunakan. Selain itu, komunikasi dengan pihak internal dan eksternal juga merupakan langkah yang penting ketika terjadinya insiden. Oleh karena itu, perencanaan awal dalam manajemen insiden dan keterlibatan pihak top management dalam setiap fase manajemen insiden sangatlah penting. Hal ini agar setiap insiden yang dialami dapat diselesaikan dengan cepat dan tepat.

4. Hasil Penelitian

Berdasarkan pada *National Cybersecurity Strategy Guide* yang diupblikasikan oleh ITU, ancaman siber dibedakan berdasarkan karakter, dampak, asal dan aktor. Ancaman yang tidak disengaja terjadi tanpa niat yang direncanakan, misalnya kesalahan sistem atau perangkat lunak dan kerusakan fisik. Namun, ancaman yang disengaja dihasilkan dari tindakan yang disengaja terhadap keamanan siber. Ancaman yang disengaja meliputi pemeriksaan rutin jaringan komputer dengan menggunakan perangkat monitoring, hingga serangan siber yang menggunakan pengetahuan sistem khusus. Ancaman disengaja yang terwujud dinamakan serangan. Sedangkan ancaman aktif merupakan

https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4
DOI: 10.7454/jkskn.v2i2.10025

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

ancaman yang mengakibatkan beberapa perubahan pada keadaan atau operasi pada suatu sistem, seperti modifikasi data, infiltrasi, dan kerusakan peralatan fisik. Sebaliknya, ancaman pasif tidak melibatkan perubahan keadaan pada peralatan. Ancaman pasif bertujuan untuk mengumpulkan informasi sebanyak-banyaknya dari suatu sistem tanpa mempengaruhi sumber daya sistem yang ada. Teknik ancaman pasif yang umum termasuk intruder, penyadapan dan analisis paket data.

Pelaku ancaman dapat digolongkan ke dalam dua subyek, yakni ancaman siber yang berasal dari state-actor maupun non-state actor. Pergerakan dari non-state actor ini dapat menimbulkan ancaman yang cukup signifikan terhadap adanya serangan/insiden siber, Non-state actor dinilai memiliki kemampuan yang lebih dalam menyebabkan kerusakan atau kehancuran pada aspek kehidupan serta mengganggu kestabilan dan keamanan nasional.

Pada tulisan ini, penulis akan melakukan analisis ancaman terhadap penerapan framework manajemen insiden. Analisis yang dilakukan menggunakan pendekatan teori ancaman yang diperkenalkan oleh Hank Prunckun (2019). Dalam teori tersebut, parameter ancaman terdiri dari dua komponen utama, yakni threat intent dan threat capability. Threat Intent merupakan optimisme dari agen lawan yang dapat menimbulkan kesuksesan ketika melakukan penyerangan. Threat Intent ini terdiri dari dua elemen, yakni elemen desire (keinginan) dan expectation (harapan). Sedangkan threat capability merupakan kekuatan dari agen lawan yang dapat diarahkan untuk melakukan serangan kepada target. Threat capability terdiri dari dua elemen, yakni knowledge (pengetahuan) dan resource (sumber daya).

Adapun mekanisme dalam melakukan analisis ancaman adalah sebagai berikut :

a. Melakukan wawancara kepada narasumber perihal elemen-elemen ancaman yang ada terhadap penerapan manajemen insiden.
b. Melakukan pengelompokan terhadap setiap elemen yang ada berdasarkan pada 4 elemen analisis ancaman.
c. Membuat survey kuesiner berdasarkan pada pengelompokan tadi dan menyebarkannya kepada 32 responden secara online.
d. Melakukan penilaian terhadap hasil kuesioner berdasarkan pada survey yang telah dilakukan. Pedoman penilaian dapat dilihat pada tabel 1.

Skala Ancaman	Nilai
Dapat diabaikan	1
Rendah	2
Menengah	3
Tinggi	4
Kritis	5

Tabel 1. Skala dan nilai ancaman
Sumber : Prunckun (2019)

e. Menjumlahkan hasil penilaian yang telah dilakukan dan menghitung rata-rata setiap elemen ancaman yang ada. Nilai ini merupakan koefisien skala ancaman.
f. Melakukan konversi nilai koefisien yang dihasilkan berdasarkan tabel 2.

Ancaman	Koefisien
Dapat diabaikan	4 – 6
Rendah	7 – 10
Menengah	11 – 15
Tinggi	16 – 18
Kritis	19 – 20

Tabel 2. Skala dan koefisien ancaman
Sumber : Prunckun (2019)

Hasil penilaian terhadap analisis ancaman terhadap penerapan manajemen insiden di Indonesia yang didapatkan dari 32 responden dapat dilihat pada tabel 3 berikut. Dilihat dari tabel tersebut, maka nilai koefisien ancaman yang dihasilkan adalah 15,86. Apabila dilakukan pembulatan ke atas, maka nilai koefissien ancaman menjadi 16. Nilai ini masuk dalam kategori High (tinggi). Tingkat keinginan

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

penyerang dalam membuat insiden di Indonesia termasuk dalam kategori tinggi, hal ini dikarenakan terdapat motif/keinginan yang sifatnya personal hingga motif politis didalamnya. Sedangkan dilihat dari harapan penyerang dalam membuat serangan/insiden cukup tinggi mengingat adanya keinginan untuk memiliki akses utama sistem, menyisipkan malware dengan tujuan tertentu, menemukan bug/celah kerawanan dari sistem, dan informasi yang bersifat rahasia milik perusahaan yang ingin diakses/dicuri oleh penyerang.

Dilihat dari sisi pengetahuan terhadap serangan, penyerang memiliki pengetahuan yang cukup memadai dan bervariasi mulai dari tingkat pemula hingga tingkat mahir. Namun, dilihat dari sisi pengetahuan terhadap proses manajemen insiden yang dilakukan di institusi/perusahaan, berdasarkan hasil wawancara, tidak seluruh bagian dalam perusahaan memiliki pemahaman yang sama terkait manajemen insiden. Hanya sebagian kecil saja yang peduli dengan proses manajemen insiden.

Terkait dengan sumber daya yang dimiliki institusi/perusahan dalam melakukan pengelolaan terhadap insiden, penilaian terhadap hal tersebut berada dalam skala tinggi. Hal ini dikarenakan tidak seluruh institusi/perusahaan menerapkan manajemen insiden dengan baik. Hanya beberapa perusahaan yang memiliki sumber daya yang memadai dan secara regulasi mewajibkan perusahaan tersebut untuk patuh terhadap pengelolaan insiden. Kondisi ini yang menyebabkan apabila terjadi serangan/insiden siber pada institusi/perusahaan yang belum memiliki sumber daya yang memadai, dampak insiden yang diakibatkan cukup massif apabila tidak diimbangi dengan strategi penanganan insiden yang baik dari pihak manajemen. Sedangkan berdasarkan hasil survey, sumber daya yang dimiliki oleh penyerang dalam membuat insiden dinilai cukup memadai. Namun sumberdaya ini akan menjadi sangat powerfull dan tidak terbatas manakala ada non-state actor yang bermain dibelakang para penyerang ini.

No	Kategori	Desire		Expectation			Knowledge	Resource
		A	B	A	B	C	A	A
1	Praktisi 1	4	5	4	5	5	5	5
2	Praktisi 2	5	5	5	5	5	5	5
3	Praktisi 3	3	4	4	3	3	2	3
4	Praktisi 4	4	4	5	4	5	4	4
5	Praktisi 5	5	4	5	4	4	4	4
6	Praktisi 6	5	5	4	4	5	4	4
7	Praktisi 7	4	2	4	4	5	5	4
8	Praktisi 8	5	4	5	3	4	3	5
9	Praktisi 9	5	5	5	5	5	5	5
10	Praktisi 10	3	4	5	5	5	5	3
11	Praktisi 11	3	4	5	5	5	4	1
12	Praktisi 12	4	5	5	4	5	4	4
13	Praktisi 13	5	5	3	5	5	3	3
14	Praktisi 14	5	5	4	4	5	3	4
15	Praktisi 15	2	4	5	4	5	3	2
16	Praktisi 16	4	5	4	4	5	4	2
17	Praktisi 17	2	5	5	5	5	3	2
18	Praktisi 18	4	3	3	5	4	4	4
19	Regulator 1	5	3	5	4	4	4	4
20	Regulator 2	3	4	4	4	4	4	3

https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4
DOI: 10.7454/jkskn.v2i2.10025

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

21	Regulator 3	4	5	5	5	5	4	3
22	Regulator 4	2	4	5	4	4	5	4
23	Regulator 5	3	5	5	4	4	4	3
24	Regulator 6	3	4	3	3	4	4	3
25	Praktisi 19	4	4	4	3	4	4	3
26	Praktisi 20	3	2	5	4	4	3	4
27	Praktisi 21	5	5	4	5	5	4	3
28	Praktisi 22	5	4	5	5	4	4	5
29	Praktisi 23	4	2	3	4	4	3	3
30	Praktisi 24	5	4	4	4	5	4	3
31	Praktisi 25	4	5	5	5	3	5	3
32	Praktisi 26	3	3	4	5	3	5	4
Jumlah		125	132	141	137	142	127	112
Rata-rata		3.91	4.13	4.41	4.28	4.44	3.968875	3.5
Rata-rata setiap elemen		4.015625		4.375			3.968875	3.5
Koefisien Ancaman		15.859375						

Tabel 2. Penilaian Analisis Ancaman
Sumber : Prunckun (2019)

5. Kesimpulan

Ancaman terhadap penerapan framework manajemen insiden di Indonesia masih belum dapat dihindarkan. Setiap elemen ancaman, baik elemen keinginan, harapan, pengetahuan, dan sumber daya, mendukung terciptanya ancaman dalam konteks yang lebih kompleks. Tidak hanya dalam ruang lingkup sebuah perusahaan/institusi saja, namun dapat merambah dalam ruang lingkup nasional apabila belum dilakukan penerapan framework manajemen insiden secara baik dan tepat. Framework juga dapat secara tidak langsung meningkatkan kapabilitas dan kesadaran keamanan dari setiap personil dalam institusi/perusahaan, sehingga nantinya dapat menambah tingkat kepercayaan masyarakat terhadap institusi/perusahaan tersebut atau bahkan pada sistem informasi yang ada di Indonesia.

Oleh karena itu, diperlukan adanya framework manajemen insiden yang dapat diimplementasukan dengan mudah di Indonesia. Sehingga diharapkan setiap institusi/perusahaan di Indonesia memiliki panduan serta prosedur yang sistematis dan komprehensif dalam melakukan proses manajemen insiden siber. Selain itu, upaya kolaboratif perlu dilakukan oleh institusi/perusahaan di Indonesia. Hal ini mengingat tidak semua institusi/perusahaan memiliki sumber daya yang memadai dalam menerapkan manajemen insiden ini. Prosesnya masih dilakukan secara parsial. Adanya upaya saling melengkapi sumber daya yang dimiliki, koordinasi penanganan insiden, kerjasama berbagi informasi tentang celah kerawanan yang berdampak pada terjadinya insiden siber, saling berbagi pengetahuan tentang penanganan insiden, dan upaya kolaboratif lain sangat diperlukan dalam upaya mengimplementasikan kerangka kerja manajemen insiden di Indonesia. Diharapkan pula dengan adanya kerangka kerja tersebut, diharapkan institusi/perusahaan tidak kesulitan dalam menerapkan proses manajemen insiden di organisasinya.

Selain itu, proses penerapan kerangka kerja manajemen insiden ini perlu didukung dengan adanya regulasi yang tepat. Apabila berbicara tentang ketahanan nasional, maka keterlibatan semua unsur baik personal maupun organisasi dalam mendukung ketahanan

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No.2, 2019

nasional sangat diperlukan. Salah satu upaya dalam mendukung hal tersebut adalah dengan melakukan penerapan manajemen insiden di institusi/perusahaannya masing-masing. Dengan adanya proses manajemen insiden yang baik, maka ketahanan nasional akan tercipta dengan sendirinya. Dan sebaliknya, apabila ada satu atau dua pihak tidak menerapkan manajemen insiden di organisasinya, maka hal tersebut dapat menjadi celah yang dapat dimanfaatkan oleh para penyerang dalam mengeksploitasi sistem maupun sumber daya yang ada untuk membuat insiden, baik dalam skala institusi maupun skala nasional. Oleh karena itu, diperlukan adanya regulasi/kebijakan yang tepat dalam mengatur penerapan kerangka kerja manajemen insiden ini.

Daftar Pustaka

Apri, Damar. 2018. *Strategi Badan SIber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia*. Universitas Indonesia : SKSG.

Creswell, John W & Vicki L.Piano Clark. (2007). *Designing and Conducting : Mixed Methods*. Research.London : Sage Publications.

Dokumen Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020-2024.

Internasional Telecommunication Union (ITU). (2011). ITU National Cybersecurity Strategy Guide.

Linkov, I., & Kott, A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. Dalam A. Kott, Cyber Resilience of Systems and Networks. New York: Springer.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Elektronik.

Sugiyono. (2013). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung : CV. Alfabeta.

Peter, dkk. (2018). Cyber Resilience and Response. *Public-Private Analytic Exchange Program*. New York : Department of Homeland Security.

Prunckun, Hank. (2019). *Counterintelligence Theory and Practice Second Edition*. USA : Rowman & Littlefield.

Prunckun, Hank. (2019). *Methods of Inquiry for Intelligence Analysis Third Edition.* USA : Rowman & Littlefield.

Rahmawati, I. (2017). *The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defence*. Jurnal Pertahanan & Bela Negara, Vol 7 Nomor 2.

Saroha, Fuad. (2019). *Strategi Mengatasi Ancaman Siber Pada Infrastruktur Informasi Kritis Nasional Dalam Mewujudkan Kedaulatan Negara Atas Ruang Siber*. Universitas Indonesia : SKSG.

Silitonga, T.P & Ali, A.H.N. (2010). *Sistem Manajemen Insiden pada Program Manajemen Helpdesk dan Dukungan TI berdasarkan Kerangka kerja ITIL V3*. Yogyakarta : Jurnal Seminar Nasional Informatika.

https://scholarhub.ui.ac.id/jkskn/vol2/iss2/4
DOI: 10.7454/jkskn.v2i2.10025