NARATIF(Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika)
Vol. 02 No. 01 Juni 2020
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

KEAMANAN INFORMASI MENGGUNAKAN PERANGKAT PRIBADI (BYOD) SELAMA PANDEMI COVID-19 MENGGUNAKAN STANDAR ISO 27001:2013 STUDI KASUS PERGURUAN TINGGI XYZ

Saepudin
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Bandung
Jl. Soekarno Hatta No 378 Bandung
saepudin@sttbandung.ac.id

Abstrak

Selama pandemi COVID-19, banyak perusahaan menerapkan karyawan mereka untuk bekerja di rumah atau yang disebut dengan work from home (WFH). Memutus rantai transmisi COVID-19 menurut WHO (World Health Organization) yang sangat efektif dengan menjaga jarak atau dikenal sebagai jarak sosial. Untuk mendukung himbauan pemerintah, karyawan setuju untuk melakukan pekerjaan di luar kantor yang sudah menggunakan teknologi informasi. Keamanan data sensitif dan kritis harus dilindungi sesuai dengan UU ITE. Keamanan sangat penting untuk perlindungan organisasi seperti kerugian finansial dan non-finansial. Institusi pendidikan tinggi telah melakukan pekerjaan yang baik dari divisi rumah atau bahkan dosen dalam hal belajar dan mengajar dengan baik dengan digital dengan melakukan beberapa aplikasi konferensi. Menurut penelitian, membawa perangkat Anda sendiri untuk melakukan pekerjaan yang terkait dengan kantor akan berdampak dan berdampak pada organisasi.

Institusi pendidikan tinggi yang telah melakukan teknologi informasi dan menempatkan infrastruktur di dalamnya yang tidak memiliki keamanan yang memadai akan berdampak buruk bagi organisasi ketika melakukan pekerjaan di rumah menggunakan perangkat mereka sendiri. Penelitian ini akan melakukan penelitian di COVID-19 college di mana ada beberapa kasus selama kerja WFH seperti menggunakan tautan atau tautan atas nama seseorang yang menurut data korban benar, sehingga korban bersedia memberikan data sensitif tanpa konfirmasi.

Berbagai cara untuk menghemat penggunaan perangkat untuk menghindari tantangan yang membahayakan organisasi. Dalam penelitian ini, laporan ini akan dilengkapi dengan melakukan wawancara dan studi literatur dengan menerapkan praktik terbaik standar ISO 27001: 2013. Dapat membuat strategi keamanan agar orang yang membawa perangkat sendiri dapat menghindari berbagai kemungkinan. Strategi keamanan yang sesuai untuk keselamatan Perguruan Tinggi XYZ dan menghasilkan rencana keamanan yang baik dari perspektif teknis serta kebijakan yang memungkinkan keamanan data yang sensitif dan baik untuk menghindari hak akses yang mudah oleh orang yang tidak bertanggung jawab. Dari hasil penelitian didapatkan rencana keamanan untuk pengguna perangkat sendiri berupa 5 kebijakan secara non teknis dan 1 kebijakan teknis

Kata kunci :
Keamanan informasi, BYOD, ISO 27001:2013, data kritis, data sensitif

Abstract

During the COVID-19 pandemy, many companies applied their employees to work at home or what is referred to as work from home (WFH). Breaking the COVID-19 transmission chain according to WHO (World Health Organization) which is very effective by maintaining distance or known as social distance. To support the government, employees agree to do work outside the office that already uses information technology. The security of both sensitive and critical data must be protected in accordance with ITE Law. Very important security for the protection of organizations such as financial and non-financial losses. Higher education institutions have done good work from home divisions or even lecturers in terms of learning and teaching well with digital by doing several conference applications. According to research, bringing your own devices to do work related to the office will have an impact and impact on the organization.

Higher education institutions that have carried out information technology and placed infrastructure in it that do not have adequate security will adversely affect organizations when doing work at home using their own devices. This research will conduct research in XYZ colleges where there are several cases during WFH work such as using links or links in the name of someone who according to the victim's data is correct, so victims willingly provide sensitive data without confirmation.

Various ways to save the use of the device to avoid the challenges that harm the organization. In this research, this report will be completed by conducting interviews and literature studies by applying the best practices of ISO 27001: 2013 standards. Can create a security strategy for people who bring their own devices can avoid various possibilities. Security strategies that are suitable for the safety of Higher Education XYZ and produce a good security plan from a technical perspective as well as policies that enable sensitive and good data security to avoid easy access rights by irresponsible people. From the research results obtained by the security plan for the user of the device itself it consists of 5 non-technical policies and 1 technical policy

Keyword :
Information Security, BYOD, ISO 27001:2013, Critical Data, Sensitive Data

I. PENDAHULUAN

WHO telah menetapkan pandemi COVID-19, sehingga berbagai organisasi di seluruh dunia menerapkan WFH (Word From Home), maksudnya karyawan diperbolehkan bekerja di rumah untuk melakukan akses ataupun apa saja untuk melakukan pekerjaannya. Tren ini sangat diapresiasi oleh berbagai belahan dunia termasuk Indonesia bagi organisasi yang telah mengadopsi teknologi informasi. Institusi perguruan tinggi sudah mulai diliburkan untuk

pencegahan penularan COVID-19. Menurut WHO *(World Health Organization)*, untuk memutus penularan COVID-19 yang paling efektif adalah diam di rumah, sedangkan bagi karyawan yang bekerja tidak bisa tinggal di rumah terus, akan tetapi ada kewajiban untuk melakukan pekerjaan sehari-hari. Bekerja di rumah harus menggunakan perangkat seperti laptop atau smartphone dan juga tablet untuk mengakses baik menggunakan hak akses dari yang rendah sampai hak akses tinggi atau istimewa. Bekerja di rumah dengan menggunakan perangkat pribadi (Bring Your Owner Device) atau disingkat menjadi BYOD akan menimbulkan masalah bagi keamanan suatu institusi atau organisasi dari berbagai ancaman yang dapat menimbulkan risiko baik finansial atau non finansial. Dalam beberapa jurnal dan artikel pada [1] [7] [11] menyebutkan bahwa bekerja dengan mengunakan perangkat pribadi atau BYOD akan menimbulkan kelemahan baru dan perlu mitigasi agar terhindar dari berbagai risiko.

Institusi perguruan tinggi XYZ sudah menerapkan teknologi informasi/sistem informasi dan telah mendukung pemerintah untuk pemcegahan penularan COVID-19 dengan memperbolehkan bekerja di rumah atau dengan istilah yang populer WFH (Work From Home). Mahasiswa sudah mulai diliburkan dan semua dosen melakukan pembelajaran jarak jauh dan melakukan tatap muka secara daring. Petugas struktural sudah mulai bekerja dirumah dan melakukan akases ataupun konfigurasi secara remot atau jarak jauh yang dilakukan dimana saja dan kapan pun dengan menggunakan perangkat sendiri baik menggunakan laptop atau smartphone juga tablet.

Selama pandemi COVID-19, WFH masih berlaku maka terjadi masalah adanya kejahatan berupa penipuan yang mengatasnamakan seseorang atau petinggi institusi dengan melakukan tautan link yang disebar ke korban, sehingga korban percaya saja karena identitas yang diberikan benar adanya. Ini adalah salah satu kasus yang tidak menutup kemungkinan akan berdampak kerugian bagi institusi baik finansial dan non finansial. Dalam penelitian ini akan melakukan strategi keamanan kebijakan teknis dan non teknis yang harus dipahami bagi karyawan khsusnya yang memiliki hak akses yang tinggi bahkan istimewa agar terhindar dari berbagai kejahatan internet yang berdampak kerugian bagi institusi. Mengamankan data sensitif atau kritis dalam institusi akan menggunakan studi literatur baik jurnal atau artikel yang berhubungan dengan masalah keamanan membawa perangkat pribadi agar dapat diminimalisir. Standar ISO 27001:2013 dipadukan untuk membantu meningkatkan keamanan secara menyeluruh berupa kebijakan baik teknis atau non teknis.

II. TINJAUAN PUSTAKA

Keamanan fisik dan lingkungan sangat diutamakan karena jika terjadi kehilangan perangkat dimana di dalamnya ada data institusi yang harus diamankan, sehingga akan merugikan organisasi. Perangkat pribadi yang hilang bisa digunakan oleh orang lain untuk tindak kejahatan. Pengamanan secara logis seperti perlindungan malware dan penggunaan firewall dan secara legislatif seperti licensi terupdate atau masih yang lama karena ini tergantung dari perangkat pribadi masing-masing [8]. BYOD membawa tantangan baru untuk perusahaan, karyawan membawa perangkat mereka sendiri ke dalam tempat kerja dan hubungkan mereka ke sumber daya perusahaan, semua perangkat harus dikelola dengan aman. Keamanan yang ada pendekatan secara luas mencakup pengumpulan informasi. Namun, pendekatan komparatif tidak menggambarkan bagaimana cara memutuskan suatu metode untuk melakukan keamanan adaptif dalam BYOD atau cara menyediakan masukan pengetahuan untuk mengadaptasi keamanan [12].

Penggunaan perangkat pribadi dalam pekerjaan menjadi tren yang tak terbantahkan. Melalui penggunaan yang tepat, ini tentu membawa manfaat bagi perusahaan dalam hal meningkatkan efisiensi kerja dan pengurangan biaya. Banyak manfaat yang dirasakan, tetapi memberikan kesulitan dalam keamanan. Sejumlah keamanan dan masalah baru muncul termasuk kontrol perangkat yang digunakan untuk mengakses data, selain waktu dan lokasi pengaksesan [13].

Karyawan menggunakan perangkat sendiri berakibat risiko yang lebih tinggi dengan mengabaikan aspek kerahasiaan, integritas, dan ketersediaan dari aset informasi organisasi. Sementara BYOD adalah tren yang jelas dan diterima di beberapa organisasi, ada sedikit penelitian tentang bagaimana kebijakan dapat mengatasi risiko keamanan informasi yang ditimbulkan oleh BYOD[14].

Sementara sebagian besar profesional TI sepakat bahwa perangkat seluler menimbulkan risiko keamanan besar, karena kurangnya kesadaran keamanan pengguna perangkat seluler bahkan kurangnya program pelatihan dari organisasi. Hasil survei terhadap 131 mahasiswa yang memasuki dunia kerja, sangat menunjukkan kurangnya kesadaran keamanan dan perlunya kesadaran dan pelatihan keamanan perangkat seluler dalam organisasi. Masalah keamanan utama dengan perangkat seluler dan membuat beberapa rekomendasi keamanan secara umum dengan berbagai kebijakan [9].

Kebijakan BYOD dibuat untuk memasukkan persyaratan khusus untuk menyelesaikan masalah perilaku pengguna dan implikasi teknis baik dibagian perangkat keras maupun lunak dari BYOD. perusahaan perlu membuat dan mempromosikan kebijakan BYOD yang sesuai untuk membuat pengguna dapat memahami tentang kebutuhan BYOD. BYOD dirancang untuk memberikan apa yang mereka inginkan dan tidak hanya menghemat biaya dan meningkatkan produktivitas dalam perspektif perusahaan[15].

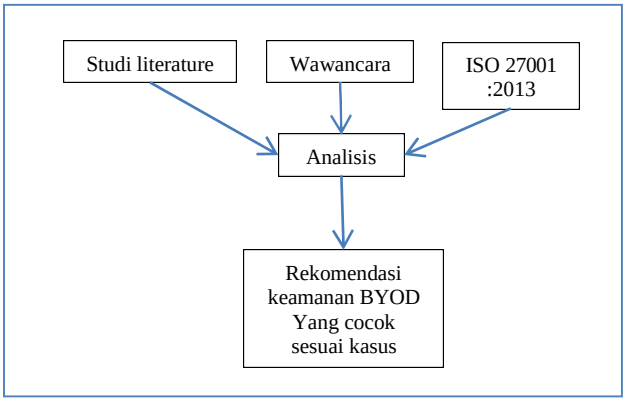
Karyawan memanfaatkan ponsel pintar miliknya sendiri dan tablet untuk bisnis. Namun, menggunakan terminal pribadi untuk bisnis menimbulkan risiko, seperti kebocoran informasi bisnis atau informasi pribadi karyawan dengan menganalisis dan mengevaluasi dengan metode manajemen risiko [16].

Ada beberapa solusi dan bertujuan untuk mengatasi keamanan BYOD dijaringan perusahaan. Solusi ini termasuk

virtual private jaringan, sistem manajemen perangkat seluler, virtual seluler mesin, dan solusi cerdas Cisco BYOD [17].

III. ANALISIS DAN PERANCANGAN

Perancangan penelitian dapat dilihat pada gambar



Gambar. 1 Alur Penelitian

Dari beberapa jurnal atau artikel bereputasi yang ada di kumpulkan dan diseleksi yang berkaitan dengan keamanan BYOD (Bring Your Owner Device) sesuai dengan permasalahan. Setelah dikumpulkan beberapa jurnal kemudian dianalisis mana yang paling berhubungan dengan masalah penelitian. Peneliti juga melakukan wawancara terhadap beberapa kunci dengan memberikan pertanyaan yang berhubungan dengan masalah penelitian. Selain wawancara dan studi literatur akan menyelesaikan permasalahan keamanan pada karyawan yang menggunakan perangkat sendiri atau pribadi dengan menggunakan kerangka terbaik sesuai dengan standar ISO 27001:2013 sehingga akan mendapatkan strategi keamanan yang paling tepat untuk menangani masalah ini.

Hasil penelusuran atikel dan jurnal yang bereputasi akan di seleksi sesuai dengan permasalahan penelitian. Pembuatan pertanyaan wawancara diambil dari praktek terbaik ISO 27001;2013 adapaun pertanyaanya dapat dilihat pada Tabel I.

TABEL I
PERTANYAAN BERDASARKAN ISO 27001

No. Klausul	Keterangan ISO 27001:2013	Pertanyaan
A.9.1.2	Akses ke jaringan dan layanan jaringan	Apakah akases ke jaringan sudah aman, seperti situs sudah terenkripsi menggunakan ? SSL/HTTPS ?
A.9.3.1	Penggunaan informasi otentikasi rahasia	Apakah pengguna sudah di beri tahu oleh manajemen bahwa data kritis dan sensitif perlu dilindungi
A.10.1.1	Kebijakan terhadap penggunaan kendali kriptograf	Apakah user atau pengguna sudah menerapkan kritografi pada perangkat seperti: minimal sudah menggunakan password untuk akses ke laptop, smartphone dan tablet?
A.11.2.1	Penempatan dan perlindungan peralatan	Apakah perangkat pribadi seperti laptop, smartphone, tablet sudah diamanakan secara fisik dari kehilangan atau pencurian ?
A.12.2.1	Kendali terhadap *malware*	Apakah laptop, smartphone dan tablet milik sendiri sudah ada anti malware?
A.12.5.1	Instalasi perangkat lunak pada sistem operasional	Apakah sudah terbaru operating sistem pada perangkat laptop, smartphone dan tablet ?

Hasil wawancara dan pertanyaan dibuat berdasarkan ISO 27001;2013 dan studi literatur akan di analisis untuk mendapatkan rekomendari strategi keamanan apa saja yang harus di buat baik rancangan praktis dan juga rancangan kebijakan dapat dilihat pada hasil dan pembahasan.

IV. HASIL DAN PEMBAHASAN

Dari hasil wawancara dengan pihak terkait dapat dilihat hasilnya dalam Tabel II

TABEL II
JAWABAN HASIL WAWANCARA

No.	Pertanyaan	Jawaban dari pihak terkait
1	Apakah akses ke jaringan sudah aman, seperti situs sudah terenkripsi menggunakan ? SSL/HTTPS ?	Sampai saat ini masih belum di implementasikan tapi sudah direncanakan, karena terkendala terjadinya pandemi COVID-19 sampai saat ini belum terlaksana
2	Apakah pengguna sudah di beri tahu oleh manajemen bahwa data kritis dan sensitif perlu dilindungi	Pada saat ini belum ada kebijakan dan arahan secara tertulis mengenai data kritis dan juga data sensitif
3	Apakah user atau pengguna sudah menerapkan kriptografi pada perangkat seperti minimal sudah menggunakan password untuk akses ke laptop, smartphone dan tablet?	Mungkin ada beberapa yang sudah menerapkan password sebelum perangkat tersebut digunakan baik laptop, smartphone atau tablet.
4	Apakah perangkat pribadi seperti laptop, smartphone, tablet sudah diamanakan secara fisik dari kehilangan atau pencurian ?, bagaimana seandainya kalau ada yang hilang dan database institusi bocor ke tangan orang jahat?	Kemungkinan besar sudah, karena saya pikir tidak ada seorangpun ingin kehilangan perangkat yang digunakan untuk pribadi, akan tetapi kalau seandainya terjadi perangkat hilang dan di dalamnya terdapat data institusi yang sangat sensitif/kritis, kemungkinan akan digunakan kejahatan oleh orang yang tidak bertanggung jawab
5	Apakah laptop, smartphone dan tablet milik sendiri sudah ada anti malware?, jika tidak ada anti malware apakah akan terjadi gangguaan pada sistem ?	Kalau perangkat mereka sendiri harusnya sudah ada dari instalasi bawaan, untuk smartphone dan tablet, juga laptop. Akan tetapi jika tidak ya akan terjadi trafik yang tidak tertangani pada sistem institusi ini
6	Apakah sudah terbaru operating sistem pada perangkat laptop, smartphone dan tablet ?	Saya tidak tahu bagi pengguna laptop akan tetapi untuk beberapa smartphone dan tablet terbaru biasanya ada update ke versi terbaru

Hasil analisis dari wawancara dengan pihak terkait menghasilkan rekomendasi keamanan dapat dilihat pada Tabel III

TABEL III
REKOMENDASI RENCANA KEAMANAN

No.	Pertanyaan	Jawaban dari pihak terkait	Rekomendasi
1	Apakah akses ke jaringan sudah aman, seperti situs sudah terenkripsi menggunakan ? SSL/HTTPS ?	Sampai saat ini masih belum di implementasikan tapi sudah direncanakan, karena terkendala terjadi pandemi COVID- 19 sampai saat ini belum terlaksana	Rencanakan untuk memasang https/SSL sebagai tindakan pengamanan untuk menghindari penyadapan, gunakanlah SSL yang berbayar karena verifikasi lebih cepat dibandingkan yang gratis
2	Apakah pengguna sudah diberi tahu oleh manajemen bahwa data kritis dan sensitif perlu dilindungi	Pada saat ini belum ada kebijakan dan arahan secara tertulis mengenai data kritis dan juga data sensitif	Segera membuat kebijakan dalam bentuk tertulis dan diketahui oleh puncak pimpinan dan merencanakan pelatihan kesadaran keamanan bagi semua karyawan
3	Apakah user atau pengguna sudah menerapkan kriptografi pada perangkat seperti minimal sudah menggunakan password untuk akses ke laptop, smartphone dan tablet?	Mungkin ada beberapa yang sudah menerapkan password sebelum perangkat tersebut digunakan baik laptop, smartphone atau tablet.	Membuat kebijakan bahwa semua karyawan yang menggunakan perangkat sendiri harus memenuhi aturan untuk menggunakan password pada laptop, smartphone dan tablet sebelum digunakan untuk menghindari jika menggunakan perangkat tanpa pengawasan
4	Apakah perangkat pribadi seperti laptop, smartphone, tablet sudah diamanakan secara fisik dari kehilangan atau pencurian ?, bagaimana seandainya kalau ada yang hilang dan database institusi bocor ke tangan orang jahat?	Kemungkinan besar sudah, karena saya pikir tidak ada seorangpun ingin kehilangan perangkat yang digunakan untuk pribadi, akan tetapi kalau seandainya terjadi perangkat hilang dan didalamnya terdapat data institusi yang sangat sensitif/kritis, kemungkinan akan digunakan kejahatan oleh orang yang tidak bertanggung jawab	Pengguna yang akan mengakses dan menyimpan data penting harus segera di hapus dari perangkat sendiri baik laptop, smartphone dan tablet jika data tersebut sudah tidak digunakan, atau gunakan enkripsi jika data tersebut masih digunakan
5	Apakah laptop, smartphone dan tablet milik sendiri sudah ada anti malware?, jika tidak ada anti malware apakah akan terjadi gangguaan pada sistem ?	Kalau perangkat mereka sendiri harusnya sudah ada dari instalasi bawaan, untuk smartphone dan tablet, juga laptop. Akan tetapi jika tidak ya akan terjadi trafik yang tidak tertangani pada sistem institusi ini	Sesegera mungkin untuk mengaktifkan anti malware dan terupdate pada perangkat pribadi seperti laptop, smartphone dan tablet, gunakan anti malware yang bagus dan berbayar
6	Apakah sudah terbaru operating sistem pada perangkat laptop, smartphone dan tablet ?	Saya tidak tahu bagi pengguna laptop akan tetapi untuk beberapa smartphone dan tablet terbaru biasanya ada update ke versi terbaru	Segera buat kebijakan agar tetap terupdate operating system yang terbaru

V. KESIMPULAN

Dari hasil penelitian didapatkan 1 kebijakan teknis dan 5 kebijakan non teknis pada institusi perguruan tinggi XYZ, Penelitian ini merupakan penelitian studi kasus sehingga tidak dapat dijadikan acuan untuk semua kondisi keamanan pada institusi tertentu meskipun kasusnya sama. Penelitian ini akan memberikan gambaran bagaimana cara mengamankan data sensitif dan kritis menggunakan perangkat milik pribadi karena kerja di rumah selama masa pandemi COVID-19,

Saran yang dilakukan untuk penelitian berikutnya adalah dapat dilakukan dengan mengacu pada beberapa standar selain ISO 27001 seperti menggunakan acuan pada kerangka COBIT 5 khusus untuk keamanan.

REFERENSI

[1] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, "Survey on access control and management issues in cloud and BYOD environment," *Int. J. Comput. Sci. Mob. Comput.*, 2017, doi: 10.14569/IJACSA.2018.091026.

[2] B. Morrow, "BYOD security challenges: Control and protect your most sensitive data," Netw. Secur., 2012, doi: 10.1016/S1353-4858(12)70111-3.

[3] A. Musarurwa, S. Flowerday, and L. Cilliers, "An information security behavioural model for the bring-your-own-device trend," SA J. Inf. Manag., 2018, doi: 10.4102/sajim.v20i1.980.

[4] A. S. Ackerman and M. L. Krupp, "Five components to consider for BYOT/BYOD," in IADIS International Conference on Cognition and Exploratory Learning in Digital Age, CELDA 2012, 2012.

[5] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and privacy considerations," IT Professional. 2012, doi: 10.1109/MITP.2012.93.

[6] G. Disterer and C. Kleiner, "BYOD Bring Your Own Device," Procedia Technol., 2013, doi: 10.1016/j.protcy.2013.12.005.

[7] S. Ali, M. N. Qureshi, and A. G. Abbasi, "Analysis of BYOD security frameworks," in Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015, 2016, doi: 10.1109/CIACS.2015.7395567.

[8] K. Hajdarevic, P. Allen, and M. Spremic, "Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments," in 24th Telecommunications Forum, TELFOR 2016, 2017, doi: 10.1109/TELFOR.2016.7818717.

[9] M. A. Harris, K. Patten, and E. Regan, "The need for BYOD mobile device security awareness and training," in 19th Americas Conference on In*formation Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, 2013.

[10] T. Oktavia, Yanti, H. Prabowo, and Meyliana, "Security and privacy

challenge in Bring Your Own Device environment: A Systematic Literature Review," in *Proceedings of 2016 International Conference on* Information Management and Technology, ICIMTech 2016, 2017, doi: 10.1109/ICIMTech.2016.7930328.

[11] R. G. Lennon, "Changing user attitudes to security in bring your own device (BYOD) & the cloud," in Proceedings - 2012 5th Romania Tier 2 Federation Grid, Cloud and High Performance Computing Science, RQ-LCG 2012, 2012.

[12] M. Amoud and O. Roudies, "Experiences in secure integration of Byod," in ACM International Conference Proceeding Series, 2017, doi: 10.1145/3134383.3134394.

[13] E. B. Koh, J. Oh, and C. Im, "A study on security threats and dynamic access control technology for BYOD, smart-work environment," in Lecture Notes in Engineering and Computer Science, 2014.

[14] D. A. Arregui, S. B. Maynard, and A. Ahmad, "Mitigating BYOD information security risks," in Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016, 2016.

[15] G. L. Boon, "A Review on Understanding of BYOD Issues , Frameworks and Policies," 3rd Natl. Grad. Conf. (NatGrad2015), Univ. Tenaga Nas., 2016.

[16] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato, and A. Kanai, "Risk assessment of BYOD: Bring your own device," in 2016 IEEE 5th Global Conference on Consumer Electronics, GCCE 2016, 2016, doi: 10.1109/GCCE.2016.7800494.

[17] Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," in 2014 IEEE 11th Consumer Communications and *Networking Conference, CCNC 2014*, 2014, doi: 10.1109/CCNC.2014.6866552.