PERSEPSI UMKM KOTA YOGYAKARTA MENGENAI *FRAUD* TEKNOLOGI INFORMASI

PERCEPTION OF MSMES IN YOGYAKARTA CITY ABOUT FRAUD OF INFORMATION TECHNOLOGY

Endang Sumirih
Prodi Akuntansi, Universitas Negeri Yogyakarta
endang.sumirih2015@student.uny.ac.id

Diana Rahmawati, S.E., M.Si.
Staf Pengajar Jurursan P. Akuntansi Universitas Negeri Yogyakarta
rahmawati_diana@uny.ac.id

Abstrak: Persepsi UMKM Kota Yogyakarta mengenai *Fraud* Teknologi Informasi. Penelitian ini bertujuan untuk mengetahui persepsi UMKM Kota Yogyakarta tmengenai *Fraud* Teknologi Informasi. Penelitian ini merupakan penelitian kualitatif. Subyek pada penelitian ini adalah UMKM Kota Yogyakarta yang telah menggunakan Teknologi Informasi. Obyek pada penelitian ini adalah Persepsi UMKM di Kota Yogyakarta. Teknik yang digunakan dalam pengumpulan data pada penelitian ini adalah wawancara yang dilaksanakan selama 20-45 menit. Teknik analisis data yang digunakan adalah teknik analisis interaktif yang meliputi pengumpulan data, reduksi data, penyajian data, kemudian penarikan kesimpulan. Validitas data yang digunakan adalah teknik triangulasi sumber. Hasil penelitian ini menunjukkan bahwa: (1) UMKM mengetahui dan paham apa itu *Fraud* Teknologi Informasi serta jenis-jenis *Fraud* Teknologi Informasi (2) UMKM sadar mengenai adanya risiko dari penggunaan Teknologi Informasi. (3) UMKM yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki cara pencegahan *Fraud* Teknologi Informasi yang sama. (4) UMKM yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki persepsi yang sama dalam tindakan penyelesaian masalah, (5) Sebagian UMKM percaya pada pihak ketiga. Namun terdapat UMKM yang tidak percaya pada pihak ketiga. (6) UMKM bersedia untuk melakukan investasi lebih untuk meningkatkan keamanan Teknologi Informasi yang digunakan. (7) Sebagian UMKM bersedia untuk melakukan perawatan rutin. Namun terdapat UMKM yang enggan untuk melakukan perawatan rutin.

Kata kunci: Persepsi, UMKM, *Fraud* Teknologi Informasi

Abstract: Perception of MSMEs in Yogyakarta City about Fraud of Information Technology. *This research has the purpose to discover the perception of MSMEs in Yogyakarta about Information Technology Fraud. This research is a qualitative research. The subjecs in this research were the MSMEs in Yogyakarta that has use Information Technology. This research object is the Perception of MSMEs in Yogyakarta City. The technique used in this research for the data collection was on interview that is held for about 20-45 minutes. For each analysis technique used is an interactive analysis technique that includes data collection, data reduction, data presentation, then drawing conclusions. The validity of the data used was source triangulation technique. This research results show that: (1) MSMEs know and understand what is Information Technology Fraud and also the types of Information Technology Fraud. (2) MSMEs knows the existence from utilizing Information Technology. (3) MSMEs that use Information Technology since the beginning of the establishment and transition business have the same method of preventing Information Technology Fraud. (4) MSMEs that use Information Technology since the beginning of the establishment and transition business have the same perception in problem solving actions. (5) Most MSMEs trust third parties. But there are MSMEs that don't trust third parties. (6) MSMEs are willing to make more investments to improve the security of Information Technology used. (7) Most MSMEs are willing to do routine maintenance. But there are MSMEs who are reluctant to carry out routine maintenance.*

***Keywords**: Perception, MSMEs, Fraud Technology Information*

PENDAHULUAN

Pada era ini para pelaku usaha makin menyadari tentang pentingnya penggunaan teknologi informasi dalam kegiatan usaha. Seiring berkembangnya teknologi informasi dan semakin ketatnya persaingan bisnis menuntut UMKM untuk memanfaatkan teknologi informasi dalam kegiatan usaha. Terdapat banyak manfaat yang dapat diperoleh dari perkembangan teknologi informasi diantaranya e-banking, ecommerce, e-trade, e-business, e-government, eeducation dan e-retailing yang dapat memudahkan masyarakat dalam melakukan aktivitasnya. Melihat dari beberapa manfaat positif, maka penggunaannya pun mulai dilakukan dengan harapan untuk menunjang operasional usahanya.

Berdasarkan penelitian Diana Rahmawati dkk (2018: 2) pemanfaatan teknologi informasi pada UMKM dinilai sudah tinggi. UMKM dinilai telah siap dalam menerapkan teknologi informasi dalam kegiatan usaha. Akan tetapi, dalam adopsi teknologi informasi oleh UMKM saat ini memiliki berbagai permasalahan yang disebabkan karena kesiapan sumber daya manusia yang masih rendah. UMKM tidak memiliki sumber daya manusia yang siap dan mampu untuk mengaplikasikannya. UMKM perlu menerapkan teknologi informasi pada usahanya agar mampu bersaing dengan kompetitor bisnis lainnya. Namun tidak dapat dipungkiri bahwa UMKM merupakan sasaran empuk kejahatan teknologi informasi karena rendahnya kesiapan sumber daya manusia. UMKM yang telah menerapkan teknologi informasi akan menghadapi berbagai risiko terkait keamanan teknologi informasi. Apabila risiko tersebut diabaikan maka akan banyak kerugian dan masalah yang dihadapi UMKM. Pada kenyataannya masih banyak UMKM yang mengabaikan hal tersebut dan menganggap bahwa teknologi informasi yang disediakan oleh pihak ketiga aman dan dapat dipercaya. Dengan demikian, UMKM menganggap perawatan rutin tidak perlu.

Umumnya, pemilik bisnis UMKM serta pegawai belum memiliki kesadaran khusus mengenai pentingnya keamanan teknologi informasi yang digunakan. UMKM menganggap bahwa pelaku kejahatan hanya akan menyerang perusahaan besar saja dan tidak mungkin menyerang bisnis mereka karena dianggap sebagai perusahaan kecil. Nation Wide melakukan survey terhadap 500 perusahaan selevel UMKM yang menunjukkan bahwa 8 dari 10 perusahaan UMKM tidak memiliki perencanaan sistem keamanan komputer (Tribunjogja, 2016: 1). Hal ini menunjukkan bahwa masih banyak UMKM yang lalai atau mengabaikan

keamanan dari teknologi informasi yang mereka gunakan. Sehingga UMKM rawan terkena kejahatan teknologi informasi.

Kejahatan teknologi informasi adalah tindakan penipuan yang ditujukan untuk memperoleh keuntungan dari korban dengan memanfaatkan teknologi informasi (Rahman dan Lackey, 2013). Tindakan *fraud* merupakan penipuan yang sengaja dilakukan oleh seseorang atau sekelompok orang sehingga menimbulkan kerugian tanpa disadari oleh pihak yang dirugikan tersebut dan memberikan keuntungan bagi pelaku kecurangan. *Fraud* umumnya terjadi karena tiga hal utama, yaitu: adanya tekanan untuk melakukan penyelewangan, adanya kesempatan yang bisa di manfaatkan serta adanya pembenaran terhadap tindakan tersebut yang dikenal dengan *fraud* triangle. (Jerry L. Turner, Theodore J. Mock, dan Rajendra P. Srivasta, 2003:16).

Fraud bisa dilakukan dengan berbagai cara, *fraud* dengan cara menyiasati sistem adalah hal yang paling sering terjadi. Tindakan ini sering dilakukan untuk mendapatkan keuntungan bagi suatu organisasi yang dilakukan baik oleh orang dalam maupun luar organisasi tersebut. Namun *fraud* sering kali dilakukan oleh sumber daya manusia yang ada dalam suatu perusahaan tersebut sehingga berdampak dapat merugikan perusahaan tersebut. Perusahaan kerap mengalami dilema menghadapi permasalahan yang melibatkan unsur orang dalam sehingga pengendalian internal dinilai harus benar-benar diperkuat. *Fraud* dapat membawa akibat kerugian financial, rusaknya reputasi, permasalahan hukum, dan operasi bisnis yang terganggu (Rahman dan Lackey, 2013).

UMKM di Kota Yogyakarta terdapat 2082 UMKM yang terdaftar di Dinas Perindagkoptan Kota Yogyakarta. (umkm.jogjakota.go.id). Telah banyak UMKM di Kota Yogyakarta yang telah mengadopsi teknologi informasi dalam menjalankan bisnis. Berdasarkan penelitian Femi Kurnia (2016: 9), terdapat 31 UMKM dari 50 UMKM yang telah menggunakan teknologi komputer, 28 UMKM yang telah menggunakan internet, dan 21 UMKM yang telah mempunyai website usaha. Dari penelitian tersebut dapat diketahui bahwa adopsi teknologi informasi oleh UMKM di Kota Yogyakarta tinggi atau telah banyak dilakukan. Akan tetapi dengan tingginya tingkat adopsi teknologi informasi oleh UMKM ini juga menimbulkan tingginya risiko yang dihadapi oleh UMKM. Risiko tersebut merupakan risiko kejahatan teknologi informasi atau *fraud* teknologi informasi. Pada tahun 2015, sebanyak 43% serangan kejahatan dunia maya mengarah pada UMKM. Hal ini disebabkan lemahnya sumber daya manusia pengguna sistem dan kurangnya keamanan pada teknologi yang digunakan (Tribunjogja, 2016: 1)

Sepanjang 2017 warga Yogyakarta banyak yang telah menjadi korban penipuan jual beli online yaitu sebanyak 80% atau 480 kasus dari 600 laporan tindak pidana ITE. Sedang selama bulan Januari 2018, polda DIY telah menerima 50 laporan tindak pidana ITE. (Liputan 6.com, Yogyakarta, 2018: 1). Pada Agustus 2018, Tokopedia telah memutus hubungan kerja (PHK) terhadap sejumlah karyawan yang diduga berlaku culas. Pemberhentian tersebut disinyalir karena dugaan praktik kecurangan dalam penyelenggaraan Flash Sale Spesial 9 pada 15-17 Agustus 2018. Terdapat beberapa karyawan yang melakukan pelanggaran transaksi terhadap 49 produk dari kampanye promosi yang dilakukan oleh Tokopedia. Dalam kasus ini menurut ahli digital forensik setidaknya terdapat dua metode yang dapat digunakan untuk melakukan *fraud* saat flash sale berlangsung. Kemungkinan pertama, yaitu pelaku membuat banyak akun anonim atau mendesain agar aksesnya lebih cepat daripada konsumen yang lain. Kemungkinan kedua, pelaku diduga membuat access list menuju IP addres yang dikehendaki. Access list ini memungkinkan hanya akun dengan server tertentu yang bisa menembus sistem Tokopedia, sedangkan IP para konsumen lain yang tidak tercantum pada daftar akan terblokir. (tirto.id, 2018: 1).

Banyaknya fenomena-fenomena *fraud* teknologi informasi pada UMKM di Kota Yogyakarta mendorong peneliti untuk melakukan penelitian ini guna mengetahui mengenai persepsi UMKM terhadap risiko *fraud* teknologi informasi yang marak terjadi di Kota Yogyakarta. Selain itu hampir sebagian besar penelitian yang dilaksanakan oleh peneliti terdahulu hanya sekedar menganalisis tentang pemanfaatan teknologi informasi oleh UMKM. Contoh Roosdhani, Wibowo, dan Widiastuti (2012: 103) menganalisis tentang tingkat penggunaan teknologi informasi oleh UMKM dan persepsi UMKM terhadap kemanfaatan teknologi informasi pada bisnis. Asril Basry dan Essy Malays Sari (2018: 53) menganalisis mengenai penggunaan teknologi informasi pada UMKM. Femi Kurnia (2016: 16) menganalisis mengenai sejauhmana pemanfaatan teknologi informasi oleh UMKM. Diana Rahmawati dkk (2018: 24) memang sudah meneliti terkait *Fraud* Teknologi Informasi tatapi penelitian tersebut masih studi eksploratori sehingga perlu studi lebih lanjut terkait dengan *Fraud* Teknologi Informasi khususnya di Kota Yogyakarta. Hal ini mendorong peneliti untuk melakukan penelitian ini untuk mengetahui persepsi UMKM mengenai *fraud* teknologi informasi dan bagaimana UMKM memandang *Fraud* Teknologi Informasi dari sudut pandang pengguna. Selain itu juga untuk mengetahui mengenai tindakan-tindakan atau pengendalian seperti apa yang perlu dilakukan oleh UMKM guna untuk

mencegah atau menanggulangi risiko *fraud* teknologi informasi yang ditimbulkan dari penggunaan teknologi informasi. Sehingga dapat digunakan sebagai acuan oleh para pelaku usaha baru ataupun UMKM yang belum menerapkan teknologi informasi.

Berdasarkan latar belakang di atas, maka peneliti menarik judul penelitian: "Persepsi Usaha Mikro, Kecil, dan Menengah (UMKM) Kota Yogyakarta mengenai *Fraud* Teknologi Informasi"

KAJIAN LITERATUR

Persepsi

Menurut Kamus Besar Bahasa Indonesia (2008:674) persepsi diartikan sebagai tanggapan (penerimaan) langsung dari sesuatu atau merupakan proses seseorang mengetahui bebarapa hal melalui panca inderanya.

Persepsi menurut Robbins dan Timothy (2008) adalah proses di mana individu mengatur dan menginterpretasikan kesan-kesan sensoris mereka guna memberikan arti bagi lingkungan mereka.

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa persepsi adalah proses di mana seseorang menginterpretasikan mengenai suatu hal terkait dengan informasi yang mereka terima.

Menurut Robbins (2003) persepsi pada umumnya dipengaruhi oleh dua faktor, yaitu faktor internal dan faktor ekstenal. Faktor internal berasal dari dalam diri individu misalnya sikap, kebiasaan dan kemauan. Sedangkan faktor eksternal adalah faktor yang berasal dari luar individu. Dijelaskan oleh Robbins (2003) bahwa meskipun individu-individu memandang pada satu benda yang sama, mereka dapat mempersepsikannya berbeda. Hal ini dipengaruhi oleh: (1) Pelaku persepsi apabila seorang individu memandang suatu obyek dan mencoba menafsirkan apa yang dilihatnya, penafsiran itu sangat dipengaruhi oleh karakteristik pribadi dari pelaku persepsi individu itu, seperti sikap, motif, kepentingan, minat, pengalaman dan harapan. (2) Obyek atau yang dipersepsikan karakteristik dari target yang akan diamati dapat mempengaruhi apa yang dipersepsikan, sasaran itu mungkin berupa orang, benda atau peristiwa. (3) Keadaan di mana persepsi itu dilakukan. Unsur lingkungan atau situasi yang terjadi saat seseorang menilai suatu obyek.

UMKM

Menurut Undang-Undang No. 20 Tahun 2008 tentang Usaha Mikro, Kecil, dan Menengah. yang disebut dengan usaha kecil adalah entitas yang memiliki kriteria sebagai berikut:

a. Kriteria Usaha Mikro adalah:

1) Memiliki kekayaan bersih paling banyak Rp 50.000.000 (lima puluh juta rupiah) termasuk tanah dan bangunan tempat usaha; atau;
2) Memiliki hasil penjualan tahunan paling banyak Rp 300,000.000 (tiga ratus juta rupiah).

b. Kriteria Usaha Kecil adalah:
1) Memiliki kekayaan bersih lebih dari Rp 50.000.000 (lima puluh juta rupiah sampai dengan paling banyak Rp500.000.000,00 (lima ratus juta rupiah) tidak termasuk tanah dan bangunan tempat usaha; atau
2) Memiliki hasil penjualan tahunan lebih dari Rp300.000.000 (tiga ratus juta rupiah) sampai dengan paling banyak Rp2.500.000.000 (dua milyar lima ratus juta rupiah).

c. Kriteria Usaha Menengah adalah:
1) Memiliki kekayaan bersih lebih dari Rp500.000.000 (lima ratus juta rupiah) sampai dengan paling banyak Rp10.000.000.000 (sepuluh miliyar rupiah) tidak termasuk tanah dan bangunan tempat usaha; atau
2) Memiliki hasil penjualan tahunan lebih dari Rp2.500.000.000 (dua milyar lima ratus juta rupiah) sampai dengan paling banyak Rp50.000.000.000 (lima puluh milyar rupiah).

Persepsi UMKM

Berdasarkan kajian teori di atas mengenai persepsi, dapat disimpulkan bahwa persepsi adalah proses di mana seseorang menginterpretasikan mengenai suatu hal terkait dengan informasi yang mereka terima.

UMKM adalah usaha produktif yang dimiliki perorangan maupun perusahaan yang telah memenuhi kriteria sebagai usaha mikro, kecil, menengah. Persepsi UMKM itu sendiri merupakan cara pandang UMKM terhadap suatu kejadian atau fenomena-fenomena yang terjadi dilingkungan mereka sesuai dengan apa yang dilihat oleh mereka. Sehingga persepsi UMKM satu dengan UMKM lainnya akan berbeda sesuai dengan apa yang mereka lihat dan perasaan atau kondisi mereka serta kondisi lingkungan mereka.

Konsep *Fraud*

Menurut Albrecht., et al (2014) *Fraud* merupakan suatu istilah yang umum dan mencakup segala macam cara yang dapat digunakan dengan kelihaian tertentu, yang dipilih oleh seorang individu, untuk mendapatkan keuntungan dari pihak lain dengan melakukan representasi yang salah.

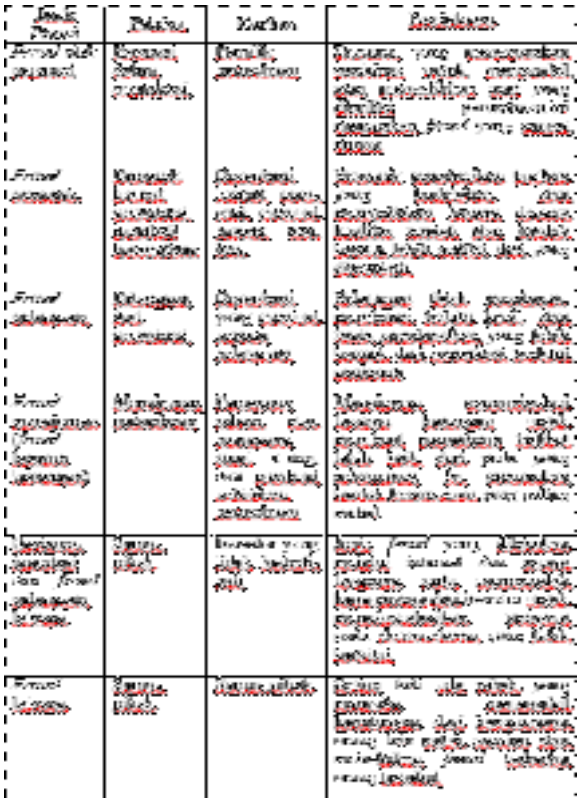
Menurut Karyono (2013: 4-5) *fraud* dapat diistilahkan sebagai kecurangan yang mengandung makna suatu penyimpangan dan perbuatan melanggar hukum, yang

dilakukan dengan sengaja untuk tujuan tertentu misalnya menipu atau memberikan gambaran keliru kepada pihak-pihak lain, yang dilakukan oleh orang-orang baik dari dalam maupun dari luar organisasi.

Berdasarkan penjelasan di atas, dapat disimpulkan *fraud* adalah suatu tindakan yang menyimpangan dan melanggar hukum, yang dilakukan dengan sengaja untuk memperoleh keuntungan dari pihak lain.

Menurut Albrecht., et al (2014) *fraud* diklasifikasikan menjadi enam jenis yaitu:

Tabel 1. Berbagai Jenis *Fraud*



Teori *Triangle Fraud*

Teori *fraud triangle* merupakan suatu gagasan yang meneliti tentang penyebab terjadinya *fraud*. Gagasan ini pertama kali diciptakan oleh Donald R. Cressey (1953) diperkenalkan dalam literatur profesional pada SAS No. 99, yang dinamakan *fraud* triangle atau segitiga kecurangan. *Fraud* triangle adalah segitiga kecurangan yang menjelaskan adanya tiga faktor yang mempengaruhi seseorang dalam melakukan tindakan kejahatan. Tiga faktor tersebut adalah sebagai berikut:

Gambar 1. Triangle *Fraud*

1. Pressure (tekanan), yaitu adanya insentif/tekanan/kebutuhan untuk melakukan *fraud*. Tekanan dapat mencakup hampir semua hal termasuk gaya hidup, tuntutan ekonomi, dan lain-lain termasuk hal keuangan dan non keuangan. Menurut SAS No. 99, terdapat empat jenis kondisi yang umum terjadi pada pressure yang dapat mengakibatkan kecurangan. yaitu financial stability, external pressure, personal financial need, dan financial targets.

2. Opportunity (kesempatan), yaitu situasi yang membuka kesempatan untuk memungkinkan suatu *fraud* terjadi. Biasanya terjadi karena pengendalian internal perusahaan yang lemah, kurangnya pengawasan dan penyalahgunaan wewenang.
3. Rationalization (rasionalisasi) yaitu adanya sikap, karakter, atau serangkaian nilai-nilai etis yang membolehkan pihak-pihak tertentu untuk melakukan tindakan *fraud*, atau orang-orang yang berada dalam lingkungan yang cukup menekan yang membuat mereka merasionalisasi tindakan *fraud*.

Teori *Coso Enterprise Risk Management-Integrate Framework* (COSO ERM)

COSO ERM adalah kerangka kinerja manajemen risiko korporasi (MRK) yang diterbitkan oleh Committee of Sponsoring Organizarions of the Treadway Commission Amerika Serikat pada tahun 2004. COSO ERM merupakann pengembangan dari kerangka kerja COSO untuk pengendalian internal yang diterbitkan pada tahun 1992. COSO ERM adalah suatu proses yang dipengaruhi oleh *broad of director*, dan personel lain dari suatu organisasi, diterapkan dalam *setting strategi*, dan mencakup organisasi secara keseluruhan, didesain untuk mengidentifikasi kejadian potensial yang mempengaruhi suatu organisasi, untuk memberikan jaminan yang cukup pantas berkaitan dengan pencapaian tujuan organisasi.

Kerangka kerja COSO ERM terdiri atas delapan komponen sebagai berikut:

a. Lingkungan Internal

   Komponen ini mengidentifikasi kondisi internal perusahaan, meliputi kekuatan dan kelemahannya, serta pandangan entitas terhadap risiko dan manajemen risiko.

b. Penetapan sasaran

   Sasaran kegiatan manajemen risiko harus sejalan dengan sasaran dari perusahaan, serta konsisten dengan risk appetite perusahaan

c. Indentifikasi kejadiaan

   Kejadian internal dan eksternal yang dapat mempengaruhi pencapaian sasaran dari perusahaan harus diidentifikasi, meliputi risiko dengan kesempatan yang dapat muncul.

d. Penilaian risiko

   Risiko dianalisis berdasarkan kemungkinan dan dampaknya. Hasil analisis risiko akan dijadikan dasar untuk menentukan perilaku risiko.

e. Perilaku risiko

   Terdapat empat alternatif pada perlakuan risiko yaitu menghindari, menerima, mengurangi, dan membagi risiko. Pemilihan perlakuan risiko dilakukan dengan membandingkan hasil

analisis risiko dengan risk appetite dan risk tolerance.

f. Aktivitas pengendalian
   Membangun dan mengimplemantasikan kebijakan dan prosedur untuk memastikan perlakuan risiko diterapkan dengan efektif.
g. Informasi dan komunikasi
   Informasi yang relevan diidentifikasi, diperoleh, dan dikomunikasikan dalam bentuk dan waktu yang tepat agar personil dapat melakukan tanggung jawabnya dengan baik.
h. Pemantauan
   Seluruh kegiatan ERM harus dipantau, dievaluasi, dan dikembangkan.

***Theory of Reasod Action* (TRA)**

Theory of Reasod Action (TRA) menjelaskan tentang perilaku yang berubah berdasarkan hasil dari niat perilaku. Niat perilaku dipengaruhi oleh norma sosial dan sikap individu terhadap perilaku. Norma sosial mendefinisikan kepercayaan individu mengenai perilaku yang normal dan dapat diterima oleh masyarakat, sedangkan sikap individu terhadap perilaku berdasarkan kepercayaan individu atas perilaku tersebut (Eagle, Dahl, Hill, Bird, Spotswood, & Tapp, 2013: 123)

Theory of Reasoned Action (TRA) pertama kali diperkenalkan oleh Martin Fishbein dan Ajzen. Teori ini menghubungkan antara keyakinan (*belief*), sikap (*attitude*), kehendak (*intention*) dan perilaku (*behavior*).

***Fraud* Teknologi Informasi**

Menurut Rahman dan Lackey (2013) Kejahatan teknologi informasi adalah tindakan penipuan yang diltujukan untuk memperoleh keuntungan dari korban dengan memanfaatkan teknologi informasi.

Menurut Diana Rahmawati dkk (2018: 9) kejahatan teknologi informasi adalah tindakan penipuan yang dilakukan untuk mengambil keuntungan dari seseorang dengan menggunakan atau memanfaatkan teknologi informasi.

Berdasarkan penjelasan di atas, maka dapat disimpulkan bahwa *fraud* teknologi informasi adalah suatu tindakan penyalahgunaan teknologi informasi untuk memperoleh keuntungan dan merugikan orang lain.

Risiko-risiko dari *Fraud* Teknologi Informasi yang harus dihadapi oleh perusahaan yang menggunakan Teknologi Informasi (Rahman dan Lackey 2013) sebagai berikut:

a. Kerugian finansial langsung yaitu kerugian aset perusahaan yang dilakukan secara langsung dengan memanfaatkan celah keamanan pada teknologi informasi.
b. Dampak terhadap reputasi atau nama baik yaitu kerugian yang akan dialami oleh perusahaan berupa kurangnya kepercayaan konsumen akibat dari

adanya *Fraud* Teknologi Informasi. Konsumen akan merasa kurang nyaman dan enggan untuk melakukan pembelian atau transaksi dengan perusahaan tersebut.

c. Dampak terhadap kinerja perusahaan yaitu dengan adanya *Fraud* Teknologi Informasi yang bisa mengakibatkan sistem yang digunakan oleh perusahaan akan mengalami masalah sewaktu-waktu sehingga dapat mengakibatkan terganggunya kegiatan usaha.

d. Bocornya data dan informasi penting perusahaan perusahaan dapat berakibat fatal bagi perusahaan. Karena data merupakan sumber daya yang dapat digunakan untuk berbagai hal. Dengan bocornya data dan informasi penting perusahaan dapat menguntungkan competitor.

Menurut Romney and Steinbart (2015: 177) ada berbagai teknik kejahatan teknologi yang sering ditemui oleh UMKM yaitu sebagai berikut:

Tabel 2. Teknik Kejahatan Teknologi yang Sering Ditemui oleh UMKM Teknik Diskripsi

Teknik	Diskripsi
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Persepsi UMKM mengenai *Fraud* Teknologi Informasi

Persepsi UMKM merupakan cara pandang UMKM terhadap suatu kejadian

atau fenomena-fenomena yang terjadi dilingkungan mereka sesuai dengan apa yang dilihat oleh mereka.

Fraud teknologi informasi adalah suatu tindakan penyalahgunaan teknologi informasi untuk memperoleh keuntungan dan merugikan orang lain.

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa Persepsi UMKM mengenai *Fraud* Teknologi Informasi adalah cara pandang dari UMKM mengenai adanya *fraud* atau tindak kejahatan yang timbul akibat pemanfaatan Teknologi Informasi yang banyak terjadi dilingkungan mereka sesuai dengan pengalaman pribadi atau berdasarkan informasi yang diterima.

Persepsi UMKM mengenai *fraud* teknologi informasi yang dimaksud adalah persepsi dari UMKM mengenai *fraud* teknologi informasi yaitu bagaimana cara pandang dari UMKM mengenai *fraud* yang muncul akibat perkembangan teknologi informasi dan bagaimana cara UMKM menghadapi kemungkinan-kemungkinan yang dapat terjadi karena adanya *fraud* teknologi informasi.

METODE PENELITIAN

Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini merupakan penelitian kualitatif. Penelitian kualitatif Menurut Sugiyono (2017), merupakan metode penelitian yang berlandaskan pada filsafat postpositivisme atau enterpretif, digunakan untuk meneliti pada kondisi obyek yang alamiah, di mana peneliti adalah sebagai instrument kunci, teknik pengumpulan data dilakukan secara trianggulasi (gabungan observasi, wawancara, dokumentasi), data yang diperoleh cenderung data kualitatif, analisis data bersifat induktif/kualitatif, dan hasil penelitian kualitatif bersifat untuk memahami makna, memahami keunikan, mengkonstruksi fenomena, dan menemukan hipotesis.

Penelitian ini bertujuan untuk mengetahui dan menjabarkan persepsi UMKM mengenai adanya *fraud* teknologi informasi dengan membandingkan persepsi UMKM yang menggunakan teknologi informasi sejak awal usaha berdiri dan UMKM yang menggunakan teknologi informasi peralihan.

Subyek dan Objek Penelitian

Subyek penelitian adalah sesuatu yang diteliti baik orang, benda atau lembaga. Subjek penelitian pada dasarnya adalah yang akan dikenai kesimpulan hasil penelitian. Subjek penelitian menurut Suharsimi Arikunto (2010: 152) adalah sesuatu yang sangat penting kedudukannya didalam penelitian, subjek penelitian harus ditata sebelum penelitian siap untuk mengumpulkan data. Berdasarkan pengertian di atas subjek dalam penelitian ini adalah UMKM di Kota Yogyakarta.

Jumlah UMKM yang ada di Kota Yogyakarta yaitu sebanyak 23.000 UMKM (Dinas Koperasi & UKM Tenaga Kerja dan Transmigrasi Kota Jogja). Pemilihan subyek didasarkan pada kriteria, yaitu UMKM Kota Yogyakarta yang sudah menggunakan Teknologi Informasi pada pembuatan laporan keuangan, data base perusahaan, penggajian, pelayanan konsumen, dan pencatatan stock barang. Berdasarkan kriteria tersebut maka peneliti mencari UMKM yang sesuai dengan kriteria, akan tetapi dari sejumlah UMKM yang sudah sesuai dengan kriteria tersebut hanya terdapat 10 UMKM yang bersedia untuk menjadi responden pada penelitian ini.

Objek penelitian merupakan permasalahan yang diteliti. Menurut Sugiyono (2009: 38) pengertian objek penelitian adalah sebagai berikut:

"Suatu atribut atau sifat atau nilai dari orang, objek atau kegiatan yang mempunyai variasi tertentu yang di tetapkan oleh peneliti untuk di pelajari dan kemudian ditarik kesimpulannya". Objek dari penelitian ini adalah Persepsi UMKM di Kota Yogyakarta. Penelitian ini dilaksanakan pada perusahaan UMKM yang terdapat di Yogyakarta. Dipilihnya UMKM yang terdapat di Kota Yogyakarta ini didasarkan pada pertimbangan bahwa perusahaan UMKM yang terdapat di Kota Yogyakarta memiliki data yang diperlukan untuk penyusunan skripsi ini.

Definisi Operasional dan Pengukuran Variabel

***Fraud* Teknologi Informasi**

Fraud Teknologi Informasi adalah suatu tindakan penyalahgunaan teknologi informasi untuk memperoleh keuntungan dan merugikan orang lain.

Fraud Teknologi Informasi yang sering terjadi antara lain;

a. Serangan *crosstie scripting* yaitu memanfaatkan kerentanan keamanan halaman situs untuk menerobos mekanisme keamanan *browser* dan menciptakan sebuah *link* berbahaya yang memasukkan kode tak diingkan dalam satu situs.
b. Kebocoran data yaitu penyalinan data milik perusahaan tanpa izin.
c. DNS *spoofing* yaitu melacak ID dari sebuah *domain name system* (DNS) (server yang mengubah sebuah nama situs web menjadi sebuah alamat IP) meminta dan membalas sebelum server DNS yang asli melakukannya.
d. *Email spoofing* yaitu membuat sebuah alamat pengiriman dan bagian lain dari sebuah kepala email seolah email tersebut berasal dari sumber lain.
e. Pencurian identitas yaitu mengambil identitas seseorang dengan mendapatkan informasi rahasia secara illegal.
f. IP *address spoofing* yaitu menciptaka paket IP dengan sebuah alamat IP palsu untuk menyembunyikan identitas

pengirim atau meniru system computer lain.

g. *Malware* yaitu perangkat lunak yang digunakan untuk melakukan tindakan berbahaya.
h. *Phising* yaitu komunikasi yang meminta penerimanya untuk mengungkapkan informasi rahasia dengan merespon sebuah email atau mengunjungi sebuah halaman situs.
i. Penipuan *round-down* yaitu memotong perhitungan bunga pada dua posisi decimal dan menempatkan jumlah potongan tersebut dalam rekening pelaku.
j. *Skimming* yaitu penggesekkan ganda suatu kartu kredit atau secara diam-diam menggesekkannya pada pembaca kartu guna mereka data untuk penggunaan selanjutnya.
k. Rekayasa social yaitu Teknik-teknik yang digunakan untuk menipu seseorang agar mengungkapkan informasi rahasia.
l. *Spamming* yaitu mengirimkan pesan-pesan yang tidak diingkan ke banyak orang pada waktu yang sama.
m. *Virus* yaitu kode yang dapat dieksekusi yang melekat sendiri pada perangkat lunak, menggandakan dirinya sendiri, dan menyebar ke system atau file lain. Ketika dipicu, ia membuat perubahan tidak sah dengan cara mengoperasilan sistem.
n. *Worm* yaitu mirip dengan virus akan tetapi lebih mengarah pada sebuah program dibandingan dengan sebuah segmen kode yang disembunyikan dalam sebuah *host* program. Secara aktif mengirimkan diri sendiri ke system lain.

UMKM

Menurut Undang-Undang No. 20 Tahun 2008 tentang Usaha Mikro, Kecil, dan Menengah. yang disebut dengan usaha kecil adalah entitas yang memiliki kriteria sebagai berikut:

Tabel 3. Kategori UMKM

Ukuran Usaha	Kekayaan Bersih	Omset
Mikro	< 50 juta	< 300 juta
Kecil	50 - 500 juta	300 juta - 2,5 milyar
Menengah	500 juta - 10 milyar	2,5 - 50 milyar

Persepsi UMKM mengenai *Fraud* Teknologi Informasi

Persepsi UMKM mengenai *Fraud* Teknologi Informasi adalah cara pandang dari UMKM mengenai adanya *.fraud* atau tindak kejahatan yang timbul akibat pemanfaatan Teknologi Informasi yang banyak terjadi di lingkungan mereka sesuai dengan pengalaman pribadi atau berdasarkan informasi yang diterima.

Beberapa indikator persepsi UMKM mengenai *fraud* teknologi informasi yang digunakan mengadopsi pada penelitian

Diana Rahmawati, dkk (2018:14) yang telah dimodifikasi:

a. Responden mengutarakan pemahamannya mengenai *fraud* teknologi informasi
b. Responden mengutarakan pemahamannya mengenai kategori *fraud* teknologi informasi
c. Responden mengutarakan pandangannya mengenai *fraud* teknologi informasi
d. Responden mengutarakan pengalamannya apabila pernah menjadi korban *fraud* teknologi informasi
e. Responden mengutarakan pengalamannya mengenai kerugian yang dialami akibat *fraud* teknologi informasi
f. Responden mengutarakan Sistem Pengendalian Internal yang digunakan dalam usahanya
g. Responden mengutarakan tindakan-tindakan yang dilakukan untuk mencegah terjadinya *fraud* teknologi informasi
h. Responden mengutarakan tindakan-tindakan yang dilakukan untuk menyelesaikan masalah yang timbul akibat terjadinya *fraud* teknologi informasi
i. Responden mengutarakan usaha yang dilakukan dalam rangka mengungguli teknologi informasi yang digunakan oleh pesaing
j. Responden mengutarakan kepercayaannya terhadap pihak ketiga yang menyediakan teknologi informasi
k. Responden mengutarakan kesediaannya berinvestasi lebih dalam meningkatkan keamanan teknologi informasi
l. Responden mengutarakan pengalaman usahanya melakukan perawatan rutin atau tidak terhadap teknologi informasi yang dimiliki

Metode Pengumpulan Data

a. Jenis Data

Pengumpulan data penelitian ini adalah dengan menggunakan data primer. Menurut Uma Sekaran (2011: 242) data primer adalah data yang diperoleh dari tangan pertama untuk analisis berikutnya untuk menemukan solusi atau masalah yang diteliti. Dalam penelitian ini data yang diperoleh langsung (data primer) berupa hasil wawancara pada perusahaan UMKM.

b. Teknik Pengumpulan Data

Pengumpulan data pada penelitian ini dilakukan dengan cara:

1. Observasi

Menurut Sugiyono (2015: 204) Metode observasi merupakan kegiatan pemuatan penelitian terhadap suatu objek. Sanafiah Faisal (1990) menglarifikasikan observasi menjadi observasi berpartisipasi, observasi terang-terangan atau tersamar dan

observasi yang tak berstruktur. Jenis observasi yang digunakan pada penelitian ini adalah observasi terang-terangan atau tersamar. Dalam melakukan observasi, peneliti memilih hal-hal yang diamati dan mencatat hal-hal yang berkaitan dengan penelitian.

2. Wawancara

Menurut Sugiyono (2016: 231) Metode wawancara merupakan teknik pengumpulan data apabila peneliti ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, tetapi juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam. Peneliti mendapatkan informasi langsung dari pemilik perusahaan UMKM dengan teknik wawancara berdasarkan kisi-kisi pedoman wawancara yang telah disusun sebelumnya. Wawancara dilaksanakan selama 20-30 menit.

Metode Analisis Data

Pada penelitian ini menggunakan teknik analisis data model Miles dan Huberman. Miles & Huberman (Sugiyono 2017: 132) menyebutkan bahwa teknik analisis data dalam peneltian kualitatif meliputi :

a. Pengumpulan Data

Mengolah dan mempersiapkan data untuk dianalisis. Langkah ini melibatkan transkrip wawancara, men-scanning materi, mengetik data lapangan atau memilah-milah dan menyusun data tersebut kedalam jenis-jenis yang berbeda tergantung pada sumber informasi.

b. Reduksi data (*Data Reduction*)

Reduksi data merupakan suatu bentuk analisis yang menggolongkan, mengarahkan, membuang yang tak perlu dan mengorganisasikan data-data yang telah di reduksi memberikan gambaran yang lebih tajam tentang hasil pengamatan menjadi tema.

c. Penyajian Data (*Data Display*)

Penyajian data merupakan analisis dalam bentuk matrik, network, cart, atau grafis. Pada penelitian kualitatif, penyajian data dilakukan dalam bentuk uraian singkat, tabel, bagan dan hubungan antar kategori. Melalui penyajian data tersebut, maka data terorganisasikan, dan tersusun sehingga akan semakin mudah dipahami.

d. Penarikan Kesimpulan (*Conclusion Drawing/Verivication*)

Kesimpulan merupakan penarikan kesimpulan dan verifikasi. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah apabila tidak ditemukan bukti-bukti kuat yang mendukung tahap pengumpulan

berikutnya. Kesimpulan dalam penelitian kualitatif dapat menjawab rumusan masalah yang dirumuskan sejak awal.

Validitas Data

Validitas data dalam penelitian ini menggunakan teknik triangulasi. Teknik triangulasi yang digunakan dalam penelitian ini adalah triangulasi sumber. Triangulasi sumber adalah membandingkan dam mengecek balik derajat kepercayaan suatu informan yang diperoleh melalui waktu dan alat yang berbeda dalam penelitian kualitatif. Hal ini dapat dicapai salah satunya dengan cara membandingkan hasil wawancara narasumber satu dengan narasumber penelitian yang lain. (Moleong, 2007: 330-331)

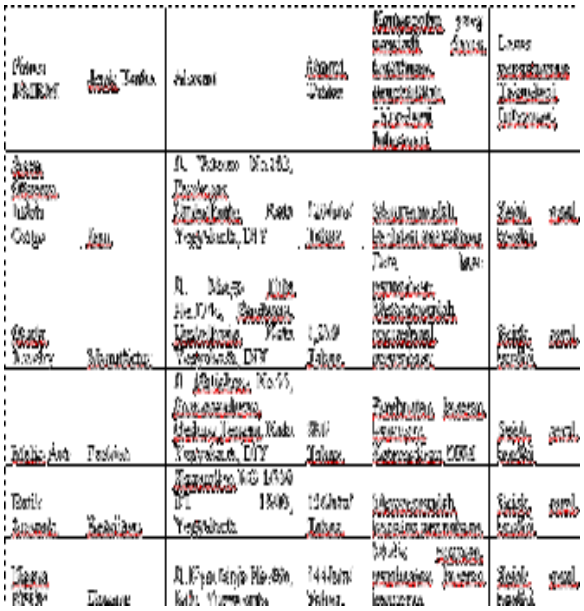
HASIL PENELITIAN DAN PEMBAHASAN

Deskripsi Data Responden

Data penelitian diperoleh melalui teknik wawancara terhadap 10 UMKM yang menjadi responden penelitian ini. Wawancara dilakukan terhadap UMKM yang dianggap representatif terhadap objek masalah dalam penelitian ini. Berdasarkan hasil perolehan data, diperoleh informasi data dari responden berupa nama usaha, jenis usaha, alamat usaha, omset usaha, keunggulan yang menjadi dasar penggunaan teknologi informasi, dan lama penggunaan teknologi informasai. Dalam penelitian ini data responden dibagi menjadi dua yaitu data responden yang menggunakan Teknologi Informasi dari awal usaha berdiri dan data responden yang tidak menggunakan Teknologi Informasi sejak usaha berdiri (peralihan).

Berikut ini data responden yang menggunakan Teknologi Informasi dari awal usaha berdiri:

Tabel 4. Data Responden yang menggunakan Teknologi Informasi Sejak Awal Berdiri



Berikut ini data responden yang menggunakan Teknologi Informasi peralihan:

Tabel 5. Data Responden yang menggunakan Teknologi Informasi Peralihan

Hasil Penelitian

Data yang diperoleh dari responden berupa jawaban responden atas pertanyaan yang diajukan oleh peneliti dengan menggunakan panduan wawancara tatap muka secara langsung, yang kemudian data penelitian tersebut disajikan dalam bentuk kutipan wawancara. Kutipan wawancara tersebut merupakan jawaban responden mengenai *Fraud* Teknologi Informasi. Peneliti menggolongkan pernyataan-pernyataan penting ke dalam beberapa kelompok tema dan membuang pernyataan-pernyataan yang kurang perlu. Pernyataan penting tersebut dikelompokkan ke dalam tujuh kelompok tema mengadopsi pada penelitian Diana Rahmawati, dkk (2018: 20) yang telah dimodifikasi:

1. Pemahaman responden tentang *Fraud* Teknologi informasi dan jenis-jenis *Fraud* Teknologi Informasi
2. Pandangan responden mengenai *Fraud* Teknologi Informasi dan kesadaran responden tentang risiko yang mungkin muncul dari penggunaan Teknologi Informasi
3. Tindakan-tindakan yang dilakukan responden untuk mencegah *Fraud* Teknologi Informasi
4. Tindakan-tindakan yang dilakukan responden untuk menyelesaikan masalah yang timbul akibat *Fraud* Teknologi Informasi
5. Kepercayaan responden kepada pihak ketiga yang menyediakan layanan Teknologi Informasi yang digunakan
6. Kesediaan responden untuk berinvestasi lebih untuk meningkatkan keamanan Teknologi Informasi yang digunakan
7. Kesediaan responden untuk melakukan perawatan Teknologi Informasi yang digunakan secara rutin.

Berikut ini merupakan tabel jawaban responden:

Tabel 6. Hasil Penelitian

Pembahasan Hasil Penelitian

1. Tema 1 (Pemahaman responden tentang *Fraud* Teknologi informasi dan jenis-jenis *Fraud* Teknologi Informasi)

   Hasil penelitian menyatakankan bahwa baik responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan sama-sama memiliki pemahaman terkait apa itu *Fraud* Teknologi Informasi serta jenis-jenis *Fraud* Teknologi Informasi yang banyak terjadi di Indonesia. Responden mampu menjelaskan dari sudut pandang mereka apa itu *Fraud* Teknologi Informasi, bagaimana *Fraud* Teknologi Informasi itu bisa terjadi, dan apa saja yang termasuk dalam jenis-jenis *Fraud* Teknologi Informasi.

   Responden berpendapat bahwa *Fraud* Teknologi Informasi adalah suatu tindakan kejahatan atau penipuan yang dilakukan melalui Teknologi Informasi untuk memperoleh keuntungan dan merugikan orang lain. Pendapat tersebut sesuai dengan pendapat Rahman dan Lackey (2013) terhadap *Fraud* Teknologi Informasi yang didefinisikan sebagai tindakan penipuan yang ditujukan untuk memperoleh keuntungan dari korban dengan memanfaatkan teknologi informasi. Responden juga memahami beberapa jenis *Fraud* Teknologi Informasi yang diidentifikasikan oleh Romney and Steinbsrt (2015: 177) seperti Malwer, Phising, Spamming, Virus, Hacking, Hoax, Cyber, Spamming, Sabotase data perusahaan, Dost, pembobolan rekening, email spoofing, manipulasi data, pencurian identitas.

   Berdasar hasil yang telah dijabarkan dapat disimpulkan bahwa pemahaman responden mengenai *Fraud* Teknologi Informasi dan jenis-jenisnya dapat dikatakan baik. Pemahaman responden mengenai *Fraud* Teknologi Informasi diharapkan dapat menjadi bekal kesiapan responden dalam menghadapi *Fraud* Teknologi Informasi yang banyak terjadi di Indonesia.

2. Tema 2 (Pandangan responden mengenai *Fraud* Teknologi Informasi dan kesadaran responden tentang risiko

yang mungkin muncul dari penggunaan Teknologi Informasi)

Hasil penelitian menunjukkan bahwa responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki persepsi yang sama. Mereka beranggapan bahwa *Fraud* Teknologi Infromasi adalah hal yang sangat mengkhawatirkan dan menakutkan karena dapat mengakibatkan kerugian bagi perusahaan. Responden juga memahami dan menyadari kemungkinan kerugiaan yang akan dialami apabila mereka menjadi korban *Fraud* Teknologi Informasi.

Responden menyatakan pendapatnya bahwa *Fraud* Teknologi Informasi dapat mengakibat kerugian material, berkurangnya kepercayaan konsumen, hilangnya data penting perusahaan, dan terganggunya kegiatan usaha. Hal ini sesuai dengan pernyataan Rahman dan Lackey (2013) terkait risiko *Fraud* Teknologi Informasi yang terdiri dari kerugian finansial langsung, dampak negatif terhadap reputasi atau nama baik, dampak negative terhadap kinerja perusahaan, serta bocornya data dan informasi penting.

Namun dengan adanya risiko-risiko tersebut tidak membuat responden enggan untuk menggunakan Teknologi Informasi dalam usahanya. Responden tetap menggunakan Teknologi Informasi untuk membantu memperlancar kegiatan usaha. Meskipun demikian. responden merasa bahwa tindakan pencegahan *Fraud* Teknologi Informasi perlu dilakukan dengan cara memahami pentingnya keamanan Teknologi Informasi, terus berhati-hati, dan mengikuti prosedur penggunaan Teknologi Informasi.

Hasil penelitian ini relevan dengan hasil penelitian sebelumnya yang dilakukan oleh Diana Rahmawati dkk (2018) yang menyatakan bahwa UMKM sadar akan risiko dann potensi masalah yang dibawa oleh pemanfaatan teknologi informasi dalam bisnis. Namun UMKM bersedia menanggung risiko karena UMKM berfikir manfaat menggunakan IT lebih besar dari pada risikonya.

3. Tema 3 (Tindakan-tindakan yang dilakukan responden untuk mencegah *Fraud* Teknologi Informasi)

Hasil penelitian menunjukkan bahwa baik perusahaan yang telah menggunakan Teknologi Informasi dari awal berdiri maupun peralihan memiliki tindakan pencegahan *Fraud* Teknologi Informasi yang hampir sama yaitu dengan melakukan pembagian jobdesk, penggunaan antivirus yang resmi, penggunaan windows yang resmi, penggunaan password dan

username/email pada laptop. Dimana password dan username hanya diketahui oleh karyawan yang memiliki keperluan akses untuk menggunakan komputer. Responden juga melakukan pengawasan kepada karyawan secara rutin. Tindakan pencegahan lain dengan melakukan update informasi dan mengikuti perkembangan Teknologi Informasi serta perkembangan *Fraud* Teknologi Informasi, rajin mengganti sandi secara berkala, melakukan *update* sistem terbaru, bertindak lebih hati-hati, melakukan *back up* data perusahaan secara berkala, dan tidak sembarangan membagikan informasi pribadi maupun informasi perusahaan pada pihak lain.

Pencegahan yang dilakukan responden bertujuan untuk mencegah terjadinya *opportunity*, yaitu situasi yang membuka kesempatan untuk memungkinkan suatu *Fraud* terjadi. Hal ini sesuai dengan teori *Fraud Triangle* yang menjelaskan bahwa faktor penyebab terjadinya *Fraud* adalah adanya *pressure*, *opportunity*, dan *rationalization*. Sehingga dapat disimpulkan bahwa hasil penelitian sesuai dengan teori *Fraud Triangle* yang diciptakan oleh Donal R. Cressey (1953). Hal ini menunjukkan bahwa responden telah memiliki kesiapan dalam menghadapi risiko penggunaan Teknologi Informasi.

4. Tema 4 (Tindakan-tindakan yang dilakukan responden untuk menyelesaikan masalah yang timbul akibat *Fraud* Teknologi Informasi)

Tindakan penyelesaian masalah yang dilakukan oleh setiap orang berbeda-beda sesuai dengan dimana letak masalah terjadi. Hasil penelitian menunjukkan bahwa baik responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun responden yang menggunakan Teknologi Informasi peralihan memiliki tindakan penyelesaikan masalah yang berbeda-beda.

Tindakan pertama yang dilakukan dalam menyelesaikan masalah yang timbul akibat *Fraud* Teknologi Informasi yaitu dengan melakukan pengecekan terlebih dahulu dimana letak masalah terjadi dan dilakukan evaluasi untuk mencari cara penyelesaian masalah tersebut. Selanjutnya diambil tindakan penyelesaian. Langkah-langkah penyelesaian risiko *fraud* yang dilakukan oleh responden sesuai dengan teori COSO ERM yang menyangkut kerangka kerja manajemen risiko perusahaan. COSO ERM terdiri dari 8 komponen yang saling terikat yaitu lingkungan internal, penetapan sasaran, identifikasi kejadian, penilaian risiko, perlakuan risiko, aktivitas pengendalian,

informasi dan komunikasi, serta pemantauan.

Hal pertama yang dilakukan responden adalah pengecekan terlebih dahulu dimana letak masalah terjadi. Responden melakukan pengecekan masalah karena terdeteksi adanya masalah *Fraud* Teknologi Informasi, proses ini merupakan identifikasi kejadian. Setelah terdeteksi adanya masalah, langkah selanjutnya dilakukan pengecekan masalah atau menelusuri masalah, proses ini merupakan penilaian risiko. Kemudian dilakukan tindakan penyelesaian, proses ini merupakan perlakuan risiko. Tindakan penyelesaian dilakukan bersamaan dengan aktivitas pengendaliaan untuk memastikan perlakuan risiko diterapkan dengan baik, dalam pelaksanaan penyelesaian juga dilakukan proses informasi dan komunikasi. Terakhir dilakukan proses pemantauan atau pengawasan seluruh kegiatan perusahaan. Sedangkan untuk lingkungan internal berkaitan dengan keadaan internal perusahaan responden, penetapan sasaran merupakan tujuan dari perusahaan responden.

Responden juga berpendapat bahwa setelah terjadi *Fraud* Teknologi Informasi maka perusahaan harus lebih berhati-hati dengan melakukan peningkatkan keamanan Teknologi Informasi yang digunakan. Sebagian besar responden memilih untuk melaporkan ke polisi apabila terjadi tindakan *Fraud* Teknologi Informasi dalam usahanya. Hal ini menunjukkan bahwa responden mengetahui tindakan yang harus mereka lakukan untuk menyelesaikan masalah yang timbul akibat *Fraud* Teknlogi Informasi.

5. Tema 5 (Kepercayaan responden kepada pihak ketiga yang menyediakan layanan Teknologi Informasi yang digunakan)

Hasil penelitian menunjukkan bahwa sebagian besar responden percaya pada pihak ketiga baik itu responden yang sejak awal usaha berdiri telah menggunakan Teknologi Informasi maupun peralihan. Hasil penelitian menunjukkan responden percaya pada pihak ketiga karena dorongan kebutuhan perusahaan untuk menggunakan Teknologi Informasi. Hal lain yang menjadi alasan responden percaya pada pihak ketiga karena pihak ketiga sudah memiliki lisensi resmi dan kredibilitas yang dapat dipertanggung jawabkan. Responden mengungkapkan bahwa pihak ketiga yang telah memiliki lisensi resmi dapat dipercaya. Sebagian besar responden percaya pada pihak ketiga karena memiliki hubungan saudara dan pertemanan dengan pihak ketiga. Responden merasa bahwa pihak ketiga tidak mungkin menjual atau membocorkan informasi mengenai

sistem yang digunakan kepada pihak lain. Karena responden kenal dekat dengan pihak ketiga maka pihak ketiga dapat dipercaya. Selain itu pihak ketiga sudah terikat kontrak dengan perusahaan. Namun terdapat beberapa responden yang berpendapat bahwa mereka tidak percaya kepada pihak ketiga dan memilihi untuk menggunakan sistem buatan sendiri. Responden merasa bahwa tetap ada kemungkinan pihak ketiga untuk membocorkan informasi atau menjual informasi perusahaan kepihak lain. Responden tidak ingin apabila pihak ketiga mengetahui seluk beluk sistem yang digunakan pada perusahaan. Hal itu membuat responden merasa kurang nyaman.

Keputusan responden untuk percaya pada pihak ketiga sesuai dengan *Theory of Reasoned Action (TRA)*, dimana kepercayaan responden dipengaruhi oleh sikap individu terhadap perilaku berdasarkan kepercayaan individu atas sikap tersebut. Pendapat responden terkait kepercayaan pada pihak ketiga juga dapat dipengaruhi oleh faktor obyek yang dipersepsikan sesuai dengan pernyataan Robbins (2003) terkait faktor-faktor yang mempengaruhi persepsi. Hasil penelitian ini relevan dengan hasil penelitian yang dilakukan oleh Diana Rahmawati dkk (2018) yang menyatakan bahwa UMKM percaya pada pihak ketiga untuk menyediakan langkah pengamanan terbaik dan UMKM fikir pihak ketiga dapat dipercaya.

6. Tema 6 (Kesediaan responden untuk berinvestasi lebih untuk meningkatkan keamanan Teknologi Informasi yang digunakan)

Hasil penelitian menunjukkan bahwa responden yang telah menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan bersedia melakukan investasi lebih untuk meningkatkan keamanan Teknologi Informasi yang digunakan. Responden merasa bahwa semakin berkembang perusahaan kebutuhan akan Teknologi Informasi juga semakin besar. Sehingga keamanan Teknologi Informasi harus lebih diperhatikan. Responden juga merasa dengan mengeluarkan biaya lebih maka keamanan Teknologi Informasi yang digunakan juga lebih baik. Sehingga perusahaan merasa lebih aman untuk menggunakan Teknologi Informasi tanpa harus khawatir data-data penting perusahaan akan bocor. Terdapat juga responden yang berpendapat bahwa apabila perusahaan memang membutuhkan dan manfaaat yang diperoleh sebanding dengan biaya yang harus dikeluarkan oleh perusahaan maka

responden bersedia untuk melakukan investasi lebih asalkan kemananan Teknologi Informasi perusahaan benar-benar terjamin.

Berdasarkan hasil penelitian dapat disimpulkan bahwa responden mempertimbangkan tingkat kebutuhan kemanan dari Teknologi Informasi itu sendiri. Responden juga mempertimbangan perbandingan antara manfaat yang diperoleh dengan biaya yang harus dikeluarkan.

Keputusan responden untuk melalukukan investasi sesuai dengan *Theory of Reasoned Action (TRA)*, dimana kepercayaan responden dipengaruhi oleh sikap individu terhadap perilaku berdasarkan kepercayaan individu atas sikap tersebut. Responden merasa bahwa keputusan mereka untuk melakukan investasi adalah benar. Hasil penelitian ini relevan dengan hasil penelitian sebelumnya yang dilakukan oleh Diana Rahmawati (2018) yang menyatakan bahwa UMKM bersedia melakukan investasi lebih asalkan mereka berfikir bahwa mereka membutuhkannya, dan biaya lebih untuk meningkatkan keamanan Teknologi Informasi harus sepadan dengan manfaat yang diperoleh.

7. Tema 7 (Kesediaan responden untuk melakukan perawatan Teknologi Informasi yang digunakan secara rutin)

Hasil penelitian menunjukkan bahwa sebagian besar responden yang telah menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan telah rutin melakukan perawatan pada Teknologi Informasi yang digunakan. Responden mengungkapkan mereka bersedia untuk melakukan perawatan rutin karena untuk menghindari terjadinya error mendadak pada sistem. Apabila terjadi error maka kegiatan usaha akan terganggu. Alasan lain karena konsumen akan menjadi kurang nyaman. Jika terjadi error mendadak maka pelayanan pada konsumen menjadi tidak maksimal dan hal itu dapat menyebabkan konsumen merasa tidak nyaman bahkan membatalkan kerjasama dengan perusahaan.

Namun tidak semua responden melakukan perawatan secara rutin. Terdapat beberapa responden yang belum melakukan perawatan secara rutin. Responden hanya melakukan perawatan saat terjadi error mendadak pada Teknologi Informasi yang digunakan perusahaan. Responden merasa bahwa perawatan rutin itu tidak perlu untuk dilakukan. Karena merasa bahwa jarang terjadi error secara mendadak dan merasa bahwa perawatan secara rutin hanya akan menambah biaya pengeluaran perusahaan. Hasil

penelitian ini sesuai dengan *Theory of Reasoned Action (TRA)*, dimana kepercayaan responden dipengaruhi oleh sikap individu terhadap perilaku berdasarkan kepercayaan individu atas sikap tersebut. Hasil penelitian ini relevan dengan hasil penelitian terdahulu yang dilakukan oleh Diana Rahmawati (2018) yang menyatakan bahwa perawatan secara rutin itu tidak dibutuhkan. Responden lebih memilih untuk melakukan perawatan isidental hanya ketika terjadi masalah pada Teknologi Informasi yang mereka gunakan.

SIMPULAN DAN SARAN

Simpulan

Berdasarkan analisis yang telah dilakukankan, dapat diketahui Persepsi UMKM mengenai *Fraud* Teknologi Informasi baik yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun pada masa peralihan dapat disimpulkan melalui 7 tema yang diteliti yaitu: Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan mengetahui dan paham apa itu *Fraud* Teknologi Informasi serta jenis-jenis *Fraud* Teknologi Informasi yang banyak terjadi di Indonesia, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki persepsi yang sama. Mereka beranggapan bahwa *Fraud* Teknologi Infromasi adalah hal yang sangat mengkhawatirkan dan menakutkan karena dapat mengakibatkan kerugian bagi perusahaan. Responden juga sadar akan adanya risiko dari penggunaan Teknologi Informasi, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki cara pencegahan *Fraud* Teknologi Informasi yang sama, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki persepsi yang sama dalam tindakan penyelesaian masalah, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan percaya kepada pihak ketiga. Namun terdapat dua Responden yang menggunakan Teknologi Informasi peralihan yang tidak percaya pada pihak ketiga, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan bersedia untuk melakukan investasi lebih untuk meningkatkan keamanan Teknologi Informasi yang digunakan, Responden yang menggunakan Teknologi Informasi sejak awal usaha berdiri maupun peralihan memiliki persepsi yang sama dalam kesedian melakukan perawatan rutin. Terdapat beberapa responden yang bersedia untuk melakukan perawatan rutin. Namun

terdapat beberapa responden yang enggan untuk melakukan perawatan rutin.

Saran

Berdasarkan hasil penelitian, berikut beberapa saran untuk penelitian selanjutnya yaitu: Hasil penelitian menunjukkan bahwa terdapat beberapa responden yang enggan melakukan perawatan rutin terhadap Teknologi Informasi yang digunakan. Berdasarkan hal tersebut perlu dilakukan sosialisasi mengenai pentingnya melakukan perawatan rutin Teknologi Informasi oleh Dinas UMKM kota Yogyakarta, Bagi peneliti selanjutnya hendaknya menambahkan jumlah responden penelitian, karena semakin banyak jumlah responden hasil penelitian cenderung lebih mendekati kenyataan yang terjadi dilapangan dan dapat menampung pendapat banyak responden, Bagi peneliti selanjutnya hendaknya menambah jumlah responden yang pernah mengalami *Fraud* Teknologi Informasi untuk mendapatkan hasil penelitian yang cenderung lebih valid.

DAFTAR PUSTAKA

Albrecht, et al. (2014). Akuntansi Forensik. Edisi Keempat. Jakarta: Salemba Empat.

Andreas, Damianus. "Metode *Fraud* yang Digunakan dalam Kasus Flash Sale Tokopedia". 04 Maret 2019. https://tirto.id/metode-*fraud*-yang-digunakan-dalam-kasus-flash-sale-tokopedia-cVpY

Arikunto. (2010). Prosedur Penelitian: Suatu Pendekatan Praktek, Jakarta: Rineka Cipta

COSO. (2004)). Enterprise Risk Management- Integrated Framework.

Dinas Koperasi dan UKM Tenaga Kerja dan Transmigrasi Kota Jogja

Eagle, et al. (2016). "Social Marketing, Pearson Education, Edinburgh Gate" . ResearchOnline@JCU

Jerry L. Turner, Theodore J. Mock, dan Rajendra P. Srivasta. (2003). An Analysis Of The *Fraud*

Karyono. (2013). Forensic *Fraud*. Edisi Kesatu. Yogyakarta: Andi.

Kurnia, Femi. (2016). "Analisis Tingkat Penggunaan Teknologi Informasi dan Komunikasi Pada Usaha Mikro, Kecil dan Menengah (Umkm) Di Yogyakarta". Repository UMY

Lexy. J, Moleong. (2007). *Metodologi Penelitian Kualitatif*. PT Remaja Rosdakarya, Bandung.

Prayudi, Yudi. "UMKM Jadi Target Baru Pelaku Cybercrime". 5 Mei 2019. http://jogja.tribunnews.com/2016/05/22/umkm-jadi-target-baru-pelaku-cybercrime

Rahman, SM, Lackey, R. (2013). "E-Commerce System Security for Small Business". International Journal of Network Security & Its Application, vol. 2, no. 2.

Rahmawati, Diana, Putritama, Afrida, Yudhiyati, Ratna, Yohan, Y.I, Kumalanisha, D.K. 2018. "Studi Eksploratori Persepsi UMKM Terhadap Kejahatan Teknologi Informasi".

Robbins, Stephen P. (2003). *Prinsip-Prinsip Perilaku Keorganisasian*. Jakarta: Erlangga.

Robbins, Stephen P. (2008). *Perilaku Organisasi.* Edisi Keduabelas. Jakarta: Salemba Empat.

Romney, M.B, and Steinbart, J.P. (2015). *Sistem Informasi Akuntansi.* Edisi 13. Jakarta: Salemba Empat.

Roosdhani, MR, Wibowo, PA, Widiastuti, A. (2012). "Analisis Tingkat Penggunaan Teknologi Informasi dan Komunikasi Pada Usaha Kecil Menengah di Kab. Jepara". Jurnal Dinamika Ekonomi dan Bisnis.

Sabandar, Switzy. "Marak, Warga Yogya Jadi Korban Kejahatan Dunia Maya". 20 Januari 2019. https://m.liputan6.com/regional/read/3269211/marak-warga-yogya-jadi-korban-kejahatan-dunia-maya

SAS NO. 99

Sekaran, Uma. (2011). Research Methods For Business. Jakarta: Salemba Empat.

Sugiyono. (2009). *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: Alfabeta.

Sugiyono. (2015). *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta.

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: Alfabeta.

Sugiyono. (2017). *Metode Penelitian Kualitatif.* Bandung: Alfabeta.

Tondi Martaon, Anggi. "ATISI Sebut Indonesia Sasaran Empuk Kejahatan Siber Dunia". 04 Maret 2019. https://www.medcom.id/teknologi/news-teknologi/GKdwB6Ek-atisi-sebut-indonesia-sasaran-empuk-kejahatan-siber-dunia

Undang-undang No. 20 tahun 2008

Website Database UMKM (umkm.jogjakota.go.id)