CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Evelyn Miyuki Ota

EDWARD SNOWDEN E WIKILEAKS:

Os Dois Lados da Moeda

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Evelyn Miyuki Ota

EDWARD SNOWDEN E WIKILEAKS:

Os Dois Lados da Moeda

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da FATEC – Americana, sob a orientação da Profa. Me. Maria Cristina Luz Fraga Moreira Aranha.

Área de concentração: Segurança da Informação.

Americana, SP
2015

Ota, Evelyn Miyuki
O96e Edward Snowden e wikileaks: os dois lados da moeda. / Evelyn Miyuki Ota. – Americana: 2015.
40f.

Monografia (Graduação em Tecnologia de Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Maria Cristina Luz Fraga Moreira Aranha

1. Segurança em sistemas de informação I. Aranha, Maria Cristina Luz Fraga Moreira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Evelyn Miyuki Ota

EDWARD SNOWDEN E WIKILEAKS:

Os Dois Lados da Moeda

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 22 de junho de 2015.

Banca Examinadora:

Maria Cristina Luz Fraga Moreira Aranha
Mestre
FATEC Americana

Raul Paiva de Oliveira
Bacharel
FATEC Americana

Henri Alves de Godoy
Mestre
FATEC Americana

AGRADECIMENTOS

Agradeço a Deus por tudo o que nos é ofertado gratuitamente todos os dias e que muitas vezes nem percebemos. Agradeço aos professores e colaboradores da FATEC, que nesses 3 anos de convivência contribuíram para a minha formação, em especial minha orientadora Maria Cristina Luz Fraga Moreira Aranha, que dispensa a seus orientandos determinação, inspiração e carinho, o que faz toda a diferença nessa jornada acadêmica.

DEDICATÓRIA

Este trabalho é dedicado à minha mãe, guerreira incansável, que acompanhou meus passos com a paciência, bondade e gentileza que são natas apenas de pais e mães.

Dedico também ao meu esposo, companheiro de longa data de outras datas, que me tornou uma pessoa melhor, me deu conteúdo e está sempre ao meu lado.

Por fim, dedico à Jordan, Bubble, Atena e Kiki, que me ensinaram amor incondicional e fizeram minha jornada terrena mais leve, bonita e alegre.

RESUMO

A segurança da informação se faz cada vez mais necessária no dia a dia da sociedade, em virtude do advento da Internet. Esta facilitou a comunicação mundial, mas, em contrapartida, implicou em maior necessidade de garantir a segurança da informação que nela transita. Esta segurança diz respeito, principalmente, ao tripé confidencialidade, integridade e disponibilidade. Assim, este trabalho teve como objetivo estudar as possíveis motivações que levam pessoas à divulgação inadvertida de informações sigilosas - como fez Edward Snowden (e diversas outras pessoas) e como ainda faz a página da Internet Wikileaks – pesquisar como a segurança da informação está sendo tratada nas corporações e o que pode ser feito para minimizar esse tipo de divulgação, já que como mostraram os resultados, o fator humano é de grande influência na segurança da informação. Esta influência é um dos principais fatores que impossibilitam extinção das falhas, como mostrado ao longo do trabalho, mas principalmente nas conclusões nele apresentadas.

Palavras chave: Confidencialidade; segurança da informação; Edward Snowden; Wikileaks.

ABSTRACT

Information security is becoming increasingly required in society on a daily basis because of Internet advent. It made global communication much easier, but in counterpart, enhanced the need to assure information security that passes through it. Such security is mainly, in regards to the tripod confidentiality, integrity and availability. Therefore, this work had as purpose to study the possible motivations that lead people to the inadvertent disclosure of classified information - like Edward Snowden did (and several other people) and Wikileaks internet web page still does - research how information security is being handled in the organizations and what can be done do minimize this sort of disclosure, once the results indicated that human is of great influence in security information. This influence is one of the main agent that unable failure extinction, as shown throughout the work, but mostly in the conclusions presented on it.

Key words: *Confidentiality*; *information security; Edward Snowden; Wikileaks.*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A rede mundial de computadores, ao passo que reduziu distâncias, aumentou a possibilidade de que informações, sigilosas ou confidenciais, sejam difundidas sem autorização (FONTES, 2006). Esse tipo de divulgação muitas vezes fica impune justamente pela dimensão da Internet, que dificulta sua identificação.

Esta característica da Internet deve-se ao fato da segurança da informação possuir diversas vulnerabilidades, como por exemplo, a existência de vírus (entre outros aspectos associados à vulnerabilidade) que podem provocar a não confidencialidade, a não integridade e a não disponibilidade que são qualidades fundamentais para a segurança da informação (FONTES, 2006). Apesar de não fazer parte do escopo deste trabalho, há ainda a engenharia social, por meio da qual é possível obter informações de toda a sorte, explorando-se a facilidade com que as pessoas são abertas a fornecer informações livremente, o que pode vir a quebrar a segurança.

Portanto, o **tema** deste trabalho relacionou-se com estudar maneiras de minimizar a divulgação de informações confidenciais.

O **escopo** do trabalho foi estudar as possíveis motivações que levaram Edward Snowden a divulgar informações confidenciais que estavam sob sua responsabilidade, o que também ocorre em empresas, os impactos na sociedade e o papel da Wikileaks, e ações para mitigar divulgações indevidas.

Segundo a página de notícias da Internet da BBC News 2013, o escândalo teve início no dia 6 de junho de 2013, quando foi publicado no jornal The Guardian e, no dia 9 de junho de 2013, Edward Snowden foi revelado como o autor dos vazamentos, no mesmo jornal.

O **problema** relacionado ao tema foi sobre a divulgação de informações sigilosas por pessoas em cargos de confiança, possuindo acesso privilegiado às informações consideradas sigilosas, que podem causar impacto danoso ou gerar sérias crises. A **pergunta** associada ao problema é: há maneiras de minimizar a divulgação de informações sigilosas que podem causar graves crises e, assim, melhorar a questão relacionada à confidencialidade.

A **justificativa** para a escolha do tema foi por este ser atual e por tratar de um assunto de interesse da sociedade como um todo, uma vez que a rede mundial de computadores é de amplo alcance, ou seja, é acessível a todas as camadas da sociedade e que, portanto, afeta a todos. O tema mostrou, também, que a questão relacionada à segurança da informação pode estar entrando em outra etapa, indicando a necessidade de tomar outros rumos, principalmente no que diz respeito ao ser humano que está ligado, direta ou indiretamente, a ela.

As **hipóteses** relacionadas ao problema e à pergunta foram:

a) O treinamento exaustivo pode ajudar, já que o que se sabe é que são poucas as pessoas que vazam informações que afetam outros países ou empresas, mas tal divulgação pode ser danosa, só para citar um dos fatores negativos associados a ela.

b) Ao mesmo tempo em que as ferramentas de segurança são desenvolvidas para proteger informações, em contrapartida, outros meios de acesso a essas informações também são descobertos.

c) O aumento do rigor das normas de segurança, implementando ferramentas para alertar sobre acessos indevidos, cópias, transferências, buscas ou alterações não autorizadas.

d) Pode haver a necessidade de outros recursos associados à segurança, uma vez que os recursos já existentes como treinamento, auditorias e atualizações não garantem 100% de segurança (ZALLIS, PENTLAND, Revista Veja, ano 48, nº10, Edição 2416, p. 17-21).

O **objetivo geral** deste trabalho foi realizar uma pesquisa sobre a divulgação de informações sigilosas e seu impacto na sociedade, contribuindo de alguma forma para auxiliar a minimizar os efeitos causados por tais divulgações.

Os **objetivos específicos** foram:

a) Pesquisar informações sobre Edward Snowden e Wikileaks, mostrando o contexto que envolvia esta pessoa e esta instituição.

b) Como ocorreram as divulgações, esclarecendo como os fatos ocorreram.

c) Propostas para mitigar divulgação de informações sigilosas, contribuindo com instituições e pessoas na orientação de condutas a serem adotadas em seus cotidianos.

Os **procedimentos metodológicos** utilizados no trabalho englobaram uma pesquisa pura, usando método hipotético dedutivo, pesquisa bibliográfica, histórica e documental, descrevendo fatos ocorridos sobre o tema abordado no trabalho. A coleta de dados foi qualitativa e quantitativa, pois além de documentos e bibliografia estudados, há a parte de gráficos estatísticos, indicando aspectos importantes, relacionados à segurança da informação. Pode ser considerada, também, uma pesquisa *ex-post-facto*, visto que só após a ocorrência das divulgações feitas e das sérias consequências provocadas por elas é que se analisou e se propôs alguma solução para situações que poderão ocorrer, semelhantes às relatadas no trabalho.

O trabalho está **organizado** da seguinte forma:

Inicia-se com a introdução, que contém um breve histórico sobre Edward Snowden e Wikileaks, suas ações e consequências, em seguida a pesquisa sobre segurança a informação (Capítulo 2) e pequisa bibliográfica (Capítulo 3), que contém estudos sobre vazamento de informações sigilosas, possíveis motivações que levaram Edward Snowden a divulgar informações confidenciais que envolviam outros países e o que a divulgação feita por ele acarretou. Além do conteúdo já citado, este trabalho apresenta formas de minimizar ações de divulgação (Capítulo 5) e o impacto que causam na sociedade, uma vez que informações sigilosas são expostas.

O estudo foi realizado usando reportagens que expuseram as informações às quais Edward Snowden tinha acesso, as consequências e acontecimentos pós-divulgação.

As conclusões apresentam as vantagens e desvantagens advindas da Internet, formas de minimizar ações de divulgação de informações sigilosas e sugestões para trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é nada mais que uma forma de proteger informações, sejam estas corporativas ou não. É baseada em três atributos:

a) Confidencialidade: propriedade que protege informações contra a revelação não autorizada ou captação compreensível;

b) Integridade: manter informações e sistemas computadorizados, dentre outros ativos, exatos e completos;

c) Disponibilidade: garantir que informações e serviços vitais estejam disponíveis quando requeridos (GASETA, 2012);

As informações estão expostas às mais diversas e variadas vulnerabilidades, tais como arquitetura de rede mal estruturada, equipamentos obsoletos ou desatualizados e também o fator humano. Os ataques, em sua maioria, poderão buscar os pontos fracos de uma rede ou mesmo pessoas que podem fornecer informações confidenciais usando de uma boa conversa persuasiva, quebrando assim um ou mais tripés do pilar da segurança da informação.

Para a proteção física e lógica existem muitos recursos como, por exemplo, portas com controle de identificação biométrica, para registro por escaneamento, as digitais ou mesmo a íris de uma pessoa, o que a tornará única em sua identificação e, portanto, apta a acessar um Data Center.

Há também Sistemas de Detecção de Intrusões (IDS), que buscam eventos ou tráfego suspeitos que são incomuns aos já registrados ou que têm uma assinatura de ataque já catalogada no IDS. Vale lembrar que o uso de um IDS requer o uso de algum tipo de Sistema de Prevenção a Intrusões (IPS), já que aquele apenas detecta, mas não tem recursos para prevenir ou tratar intrusões. Esta combinação (IDS + IPS) torna-se onerosa para as empresas, na maioria das vezes. Por este motivo muitas organizações preferem adotar alternativas para auxiliar na segurança de suas informações (ALEVATE, 2014).

Os *firewalls* são uma forma de proteção que utiliza regras e filtros de tráfego estabelecidos entre duas redes. Estas regras e filtros são configurados de forma a

exigir algum tipo de autenticação de rede, ou seja, o acesso só é permitido a usuários cadastrados.

E a criptografia garante que os dados permaneçam confidenciais já que são codificados de forma a ficarem ilegíveis a quem não possuir a chave de decodificação (KUROSE; ROSS, 2010).

2.1 PESQUISA SOBRE SEGURANÇA DA INFORMAÇÃO

Uma pesquisa realizada pela Pricewaterhouse Coopers[1] (PwC) afirma que os incidentes de segurança estão no topo das preocupações dos consumidores, ou seja, já não são exclusividade das organizações, uma vez que as informações furtadas podem afetar desde um simples cidadão até um governo inteiro.

Um dos recentes ataques mais notórios ocorreu nos Estados Unidos em agosto de 2014, chamado de *Heartbleed defect*, ou defeito do coração que sangra. Esse ataque afetou dois terços dos servidores mundiais, impactando *e-mails*, redes sociais e páginas da Internet tais como páginas de compras, aplicações de segurança dentre outros, sendo que o primeiro ataque foi a um hospital, no qual houve o furto de 4,5 milhões de registros de pacientes. Além disso, de acordo com a pesquisa, já não é mais surpresa que o crescimento dos incidentes de segurança aumenta ano após ano devido às elevadas falhas de segurança (PWC, 2015).

A Figura 1 a seguir ilustra o número de incidentes de furtos registrados pela pesquisa da PwC, ocorridos desde o ano de 2009 até 2014 que, segundo a taxa de crescimento anual composto, cresceram cerca de 66%.

[1] Pricewaterhouse Coopers é uma empresa global, na qual firmas separadas e independentes trabalham de forma integrada na prestação de serviços de assessoria tributária e empresarial e de auditoria.

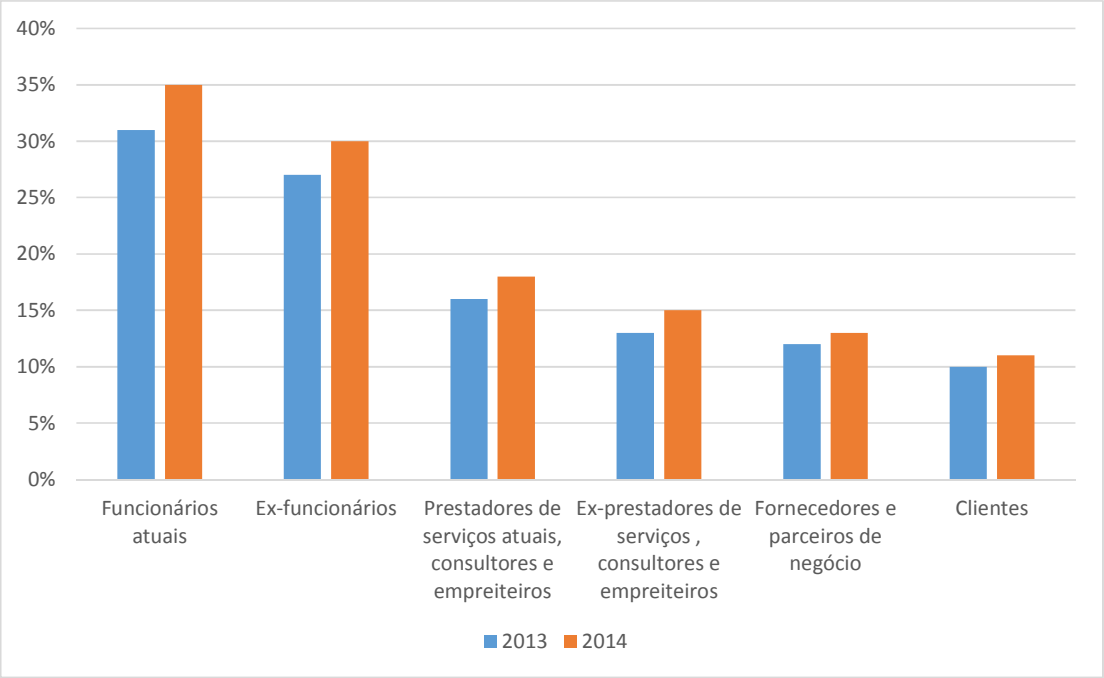
Figura 1: Gráfico de número de incidentes por ano

Fonte: (PWC, 2015)

Em tempo, segundo a mesma pesquisa, os funcionários são os maiores responsáveis pela ocorrência desses incidentes, que, em muitos casos, acabam acontecendo pela perda de dispositivos móveis ou por técnicas de persuasão de um engenheiro social, o que coloca novamente em questão o fator humano na segurança da informação.

A Figura 2 mostra os casos específicos de incidentes de segurança causados por pessoas pertencentes à organização (confirmando, novamente, a questão da relação segurança da informação em contraposição ao fator humano que trabalha com TI, tendo, portanto, algum tipo de acesso às informações). Também apresenta questões relacionadas à segurança da informação, envolvendo parceiros de negócios, ex-parceiros, ex-funcionários, fornecedores, clientes, consultores, empreiteiros, ex-prestadores de serviços, entre outros.

Figura 2: Gráfico sobre a porcentagem de incidentes de segurança causados por pessoas da organização



Fonte: (PWC, 2015)

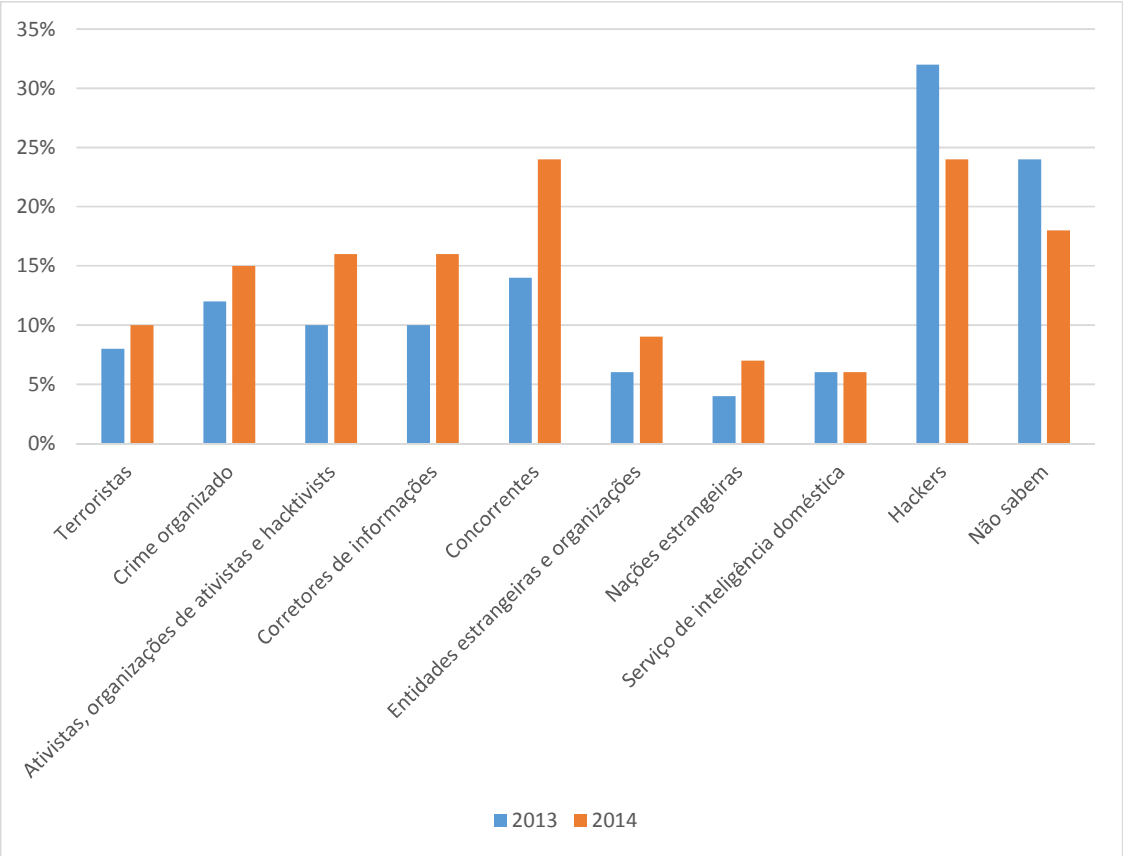
O que chama a atenção é que a porcentagem maior na Figura 2 se refere a funcionários atuais, ou seja, é o fator humano atuando nestas ocorrências. Isto pode ser explicado pelo fato de que estes, muitas vezes, causam incidentes por insatitisfação profissional, vazando informações para concorrentes, fazendo *download* de arquivos não autorizados/homologados pela empresa porque pensam que o delito não será descoberto, dentre outros (PRADO; SOUZA, 2014).

A PwC ainda informa que, de acordo com as pessoas que participaram da pesquisa, os crimes cometidos por funcionários da empresa são mais onerosos porque não possuem uma política de segurança para incidentes que envolvam seus próprios funcionários e, por isso, não estão preparados para lidar com o problema depois de ocorrido nem com sua prevenção. Este resultado confirma o que Alevate apresenta em seu livro, ou seja, incidentes internos são mais frequentes e mais onerosos que incidentes externos (ALEVATE, 2014).

Além disso, há, ainda, as invasões provocadas por pessoas de fora das organizações (chamados de incidentes externos). Desta forma, a PwC realizou uma

pesquisa para incidentes de roubos e furtos causados por pessoas que não fazem parte de alguma organização como mostra a Figura 3.

Figura 3: Gráfico sobre a porcentagem de incidentes de segurança causados por pessoas que não fazem parte da organização



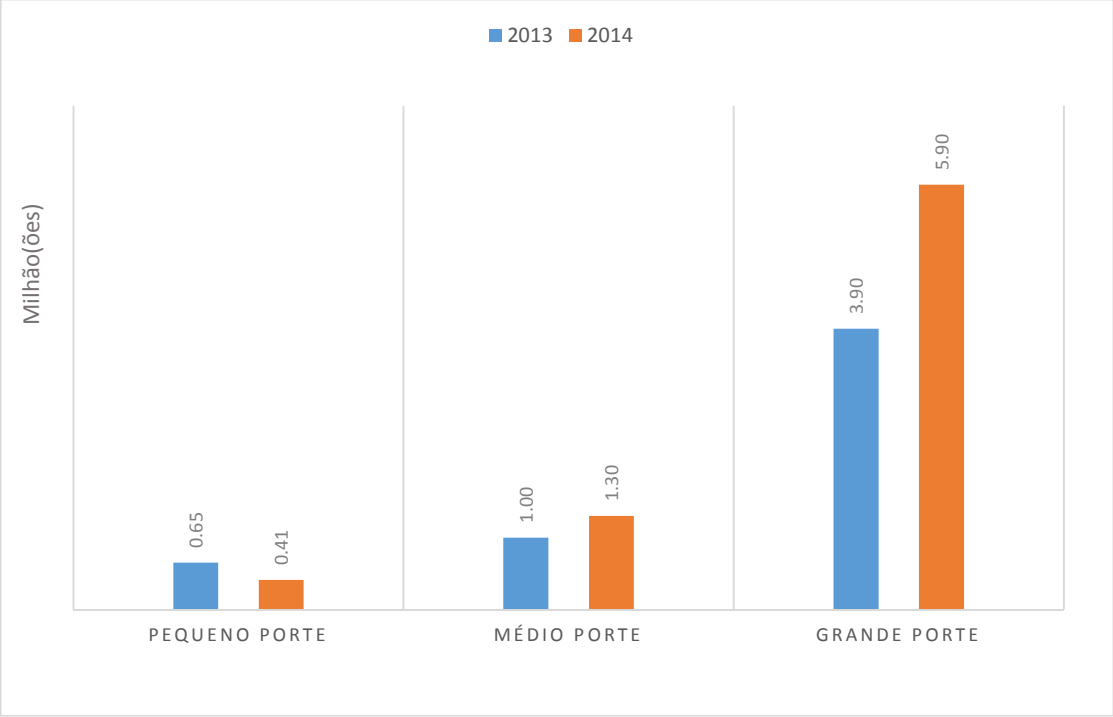
Fonte: (PWC, 2015)

Em 2013, a maior porcentagem de invasões (cerca de 33%), foram causadas por *hackers*, enquanto que em 2014, quase 25% foram causadas por concorrentes e *hackers*, cada um. Este resultado mostra que, apesar de medidas de segurança cada vez mais rigorosas, adotadas pelas organizações não alcançam o efeito desejado, que é mitigar os incidentes de segurança. Mesmo com essas medidas eles têm aumentado, conforme resultados da pesquisa feita pela PwC.

Os números são altos, mas evidenciam, de certa forma, o quanto o funcionário interno à empresa é ainda mais danoso, já que a porcentagem de incidentes causados por estes é de cerca de 35% (Figura 2), quase 10% a mais que os *hackers* (Figura 3).

As perdas financeiras causadas por incidentes de segurança mostram-se maiores nas grandes empresas[2] como mostrado na Figura 4, onde a concentração de pessoas é maior, o que também reforça que a atuação humana é muito importante na questão da segurança da informação. Os números seriam ainda mais assustadores se incluíssem os incidentes não registrados, isso porque muitas empresas não o fazem por razões estratégicas, a fim de não impactar o negócio, ou porque não estão cientes ou porque o governo está investigando. Aliás, a pesquisa também revela que as empresas muitas vezes não envolvem a justiça ou processam seus funcionários legalmente, assim, outras empresas que vierem a contratar esses mesmos funcionários, não estarão cientes dos riscos que correm ao fazer a contratação.

Figura 4: Média de perdas financeiras causadas por incidentes de segurança



Fonte: (PWC, 2015)

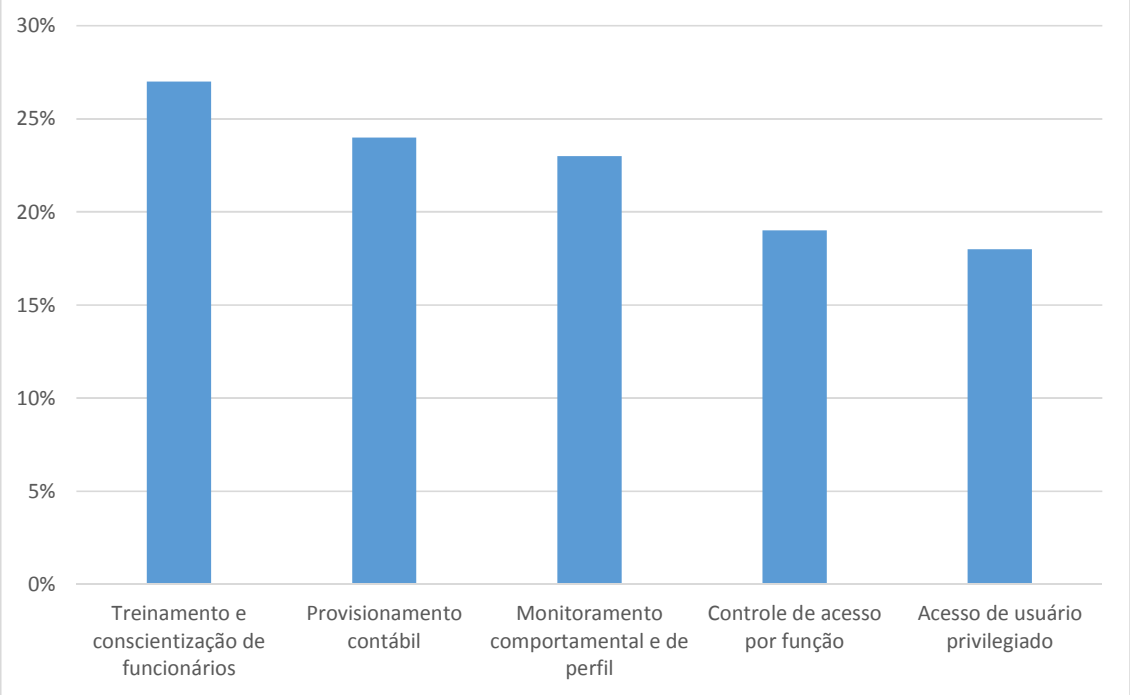
Outro ponto importante citado na pesquisa da PwC é a chamada inteligência doméstica. O fato de Edward Snowden ter revelado que a população e as organizações como um todo vêm sendo monitoradas, fez com que estes se

[2] Segundo a página de Internet do SEBRAE, para o ramo de atividade de comércio e serviços, a definição do porte de empresas é feito de acordo com o número de empregados e faturamento bruto, sendo considerada empresa de pequeno porte: de 10 a 49 empregados e faturamento de R$ 240 mil a 2,4 milhões; médio porte: de 50 a 99 e grande porte: de 100 ou mais empregados. O faturamento bruto para classificação de empresas de médio e grande porte não é informado.

preocupem mais com a sua privacidade. Fato é que algumas companhias já reconsideram a compra de equipamentos de determinados países e fabricantes. Esse comportamento, derivado das revelações de Edward, já é chamado de Efeito Snowden, visto que tais revelações ajudaram as pessoas a entender o conceito de *Big Data*[3].

Com toda sorte de vantagens e riscos que a Internet traz, as organizações têm investido não só em tecnologia para aumentar a segurança, mas também em treinamento e conscientização de funcionários. Isto pode ser constatado na Figura 5: pouco mais de 25% de investimento é para este fim (ou seja, mais de ¼ do valor investido em segurança), bem como o monitoramento comportamental e de perfil de funcionário.

Figura 5: Prioridades de investimento para prevenção de incidentes de segurança



Fonte: (PWC, 2015)

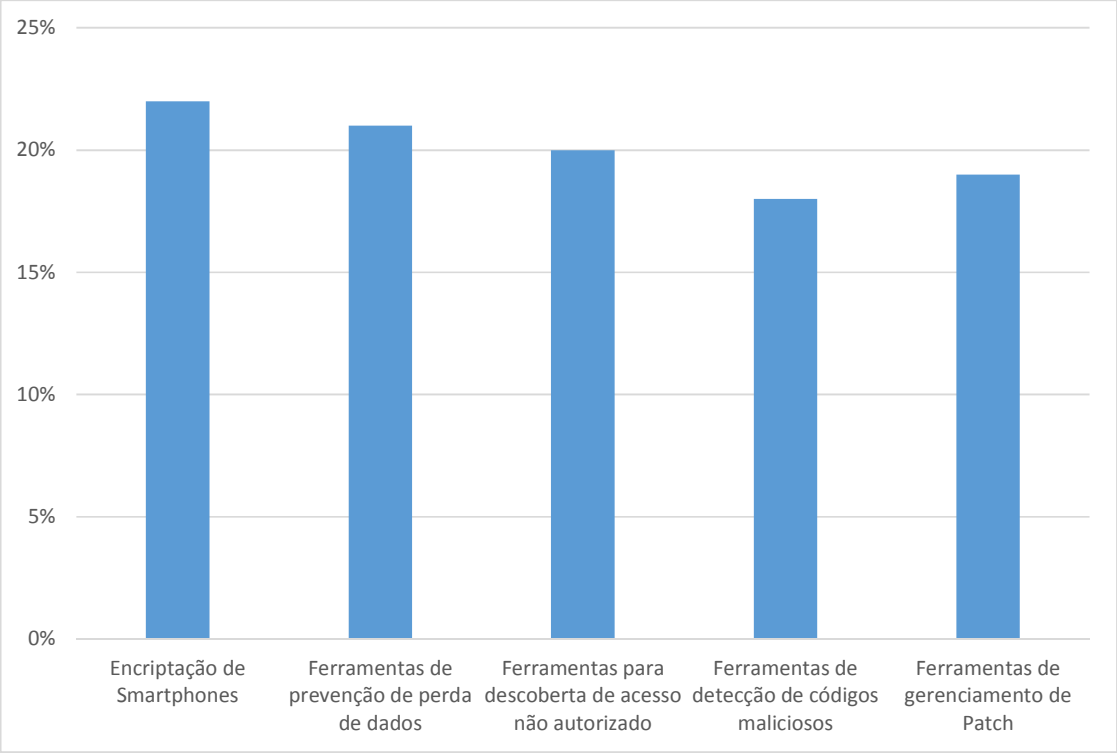
Considerando os aspectos medidos pela pesquisa, cujos resultados são apresentados na Figura 5, quatro deles (em um total de cinco aspectos) estão relacionados às pessoas. É um resultado significativo, pois as organizações

[3] Big Data é um conjunto de dados muito amplo que necessita de ferramentas específicas para analisar tais dados.

reconhecem que o fator humano é de alto risco quando o assunto é segurança da informação. Somando-se todos os percentuais de investimento mostrados na Figura 5, verifica-se que os investimentos em segurança da informação, relacionados às ações de colaboradores das organizações é alto.

A Figura 6 mostra os investimentos em proteção contra incidentes de segurança. Pode-se notar que a encriptação de *smartphones* recebe maior investimento, quase ¼, que pode ser explicado pela mobilidade do dispositivo, o que aumenta as chances de perda ou furto de dados.

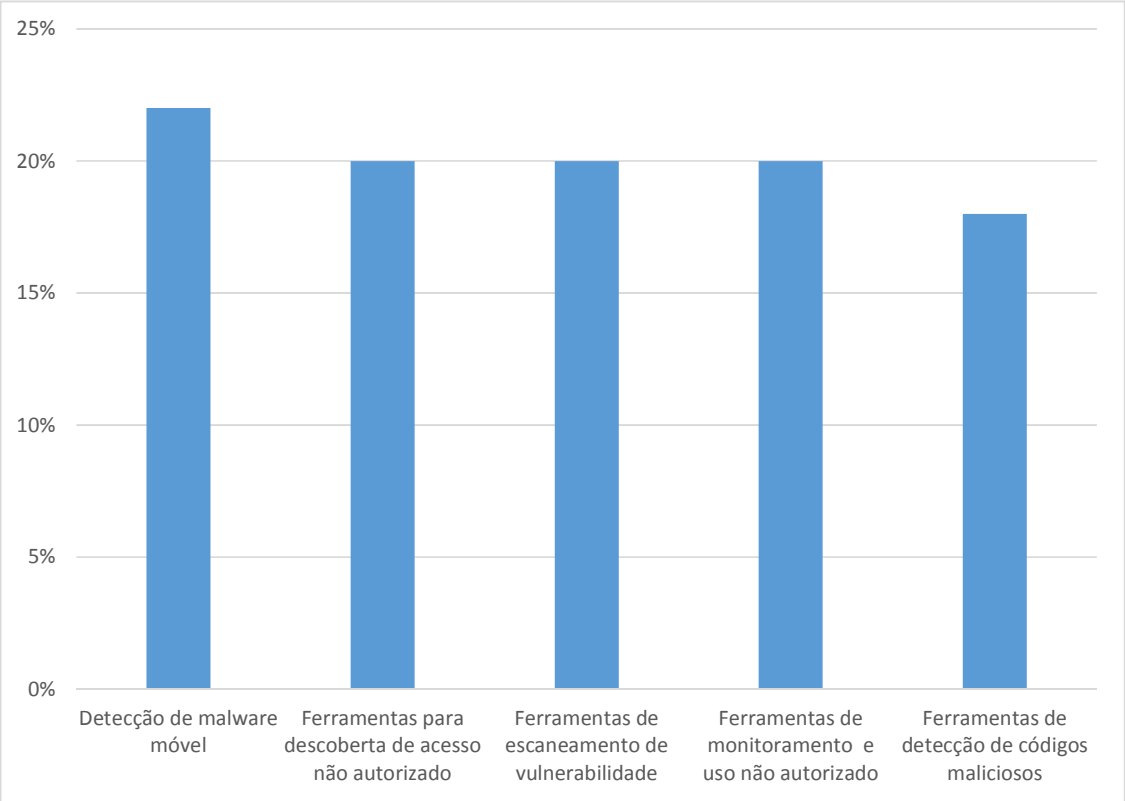
Figura 6: Prioridades de investimento para proteção contra incidentes de segurança



Fonte: (PWC, 2015)

Da mesma forma, o investimento na detecção de *malware*[4] móvel, como mostrado na Figura 7, também é um pouco maior que em ferramentas para descoberta de acesso não autorizado, escaneamento de vulnerabilidade, monitoramento e uso não autorizado e detecção de códigos maliciosos, cujos investimentos são, de certa forma, equilibrados. O *malware* móvel pode ser mais danoso, pois se instala em sistemas operacionais de dispositivos móveis.

Figura 7: Prioridades de investimento para detecção de incidentes de segurança

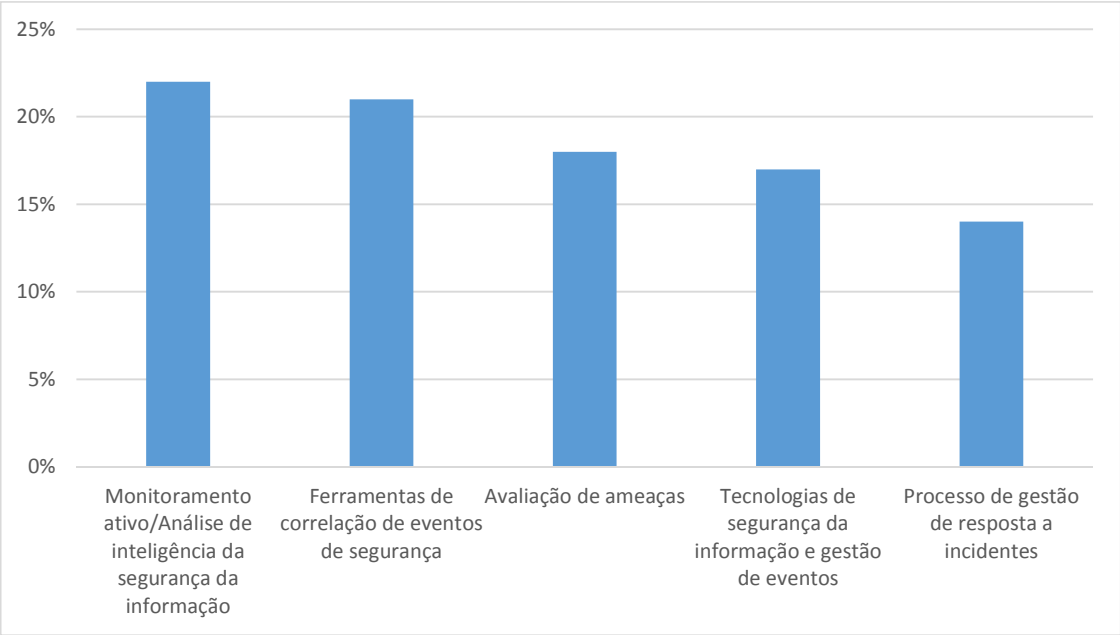


Fonte: (PWC, 2015)

[4] Segundo a página de Internet cert.br, *malware* são programas desenvolvidos como o fim de executar ações danosas em um computador.

Já para as prioridades de investimento para resposta a incidentes de segurança, a Figura 8 mostra que o monitoramento ativo e análise de inteligência da segurança da informação é o atributo que mais recebe investimento, segundo a pesquisa da PwC.

Figura 8: Prioridades de investimento para resposta a incidentes de segurança



Fonte: (PWC, 2015)

Segundo o jornal O Estado de São Paulo, houve crescimento de 88% no registro de crimes virtuais no Brasil em dois anos. Tais crimes incluem, dentre outros, o vazamento de fotos e vídeos íntimos, o que configura, mais uma vez, a quebra de confidencialidade. Uma das notícias informa sobre o funcionário de uma operadora de telefonia, que usou informações cadastrais de clientes para assediar algumas dessas clientes. Fazia isso por intermédio de um aplicativo de celular e, segundo uma das vítimas, o funcionário se recusava a apagar seu número. Com a divulgação do assédio em uma rede social, a operadora demitiu o funcionário por usar das informações de clientes que deveriam ser mantidas sob sigilo (REOLOM, O Estado de São Paulo, p. E1, 16 maio 2015).

3 EDWARD SNOWDEN E WIKILEAKS

Edward Snowden e Wikileaks fazem parte da nova geração de delatores do século 21, que se utilizam do grande alcance da Internet e também da facilidade que esta proporciona em encobrir os rastros de quem fornece as informações que deveriam estar sob sigilo.

Enquanto Snowden decidiu revelar informações secretas da Agência de Segurança Nacional (NSA) dos Estados Unidos por meio do jornal *The Guardian*, o Wikileaks (2007) o faz através de sua página na Internet, na qual inclusive apresenta uma seção que leva à outra página cujo intuito é ajudar na libertação de Edward Snowden.

Vale lembrar que vários aspectos de segurança da informação foram quebrados ao longo deste processo como, por exemplo, a quebra de sigilo contraria a premissa de confidencialidade, uma das qualidades exigidas no assunto presente em segurança da informação.

3.1 EDWARD SNOWDEN

Edward Snowden é um ex-funcionário terceirizado da NSA, nasceu na Carolina do Norte de uma família de classe média baixa. Seus pais foram funcionários públicos federais, daí seu interesse em trabalhar junto ao governo como forma de dar sua contribuição ao país que sofreu com os ataques de 11 de setembro de 2001. Com a intenção de ajudar a população do Iraque a se libertar do jugo que vinha sofrendo, Snowden alistou-se no exército em 2004, mas não durou muito, pois, após algumas semanas, sofreu um acidente e quebrou as duas pernas, fato que o forçou a sair do exército, onde também já estava desiludido, uma vez que percebeu que seu propósito de libertação era o oposto do que ele ouvia nos treinamentos, no qual se falava mais em matar pessoas do que ajudá-las.

A partir de então foi trabalhar em um órgão do governo estadunidense e apesar de não ter diploma do ensino médio, sua capacidade intelectual permitiu que conseguisse se desenvolver em serviços de tecnologia, alcançando uma posição na Universidade de Maryland e posteriormente já na *Central Intelligence Agency* (CIA). Frustrou-se com a forma como eram conduzidas algumas investigações, citando uma

ocasião em que um sujeito teve a vida destruída por um agente da CIA por algo que não deu resultado. Embriagaram o sujeito propositadamente e o encorajaram a voltar para casa dirigindo. Depois foi criada uma situação de *blitz* policial, à qual o sujeito se livraria se passasse informações confidenciais de um banco suíço. Não havendo cooperação, foram embora abandonando o sujeito à própria sorte.

Os dias no exército e os acontecimentos vivenciados na CIA contribuíram para que ele começasse a pensar em tornar públicas as informações que julgou serem de interesse público pelos comportamentos questionáveis que presenciou, como o caso da blitz policial já citada, nos idos de 2009. Não fez a delação nessa época, pois esperava que o governo de Barack Obama acabasse com esses abusos, mas após alguns anos concluiu que o que acontecia era exatamente o oposto. Até a data da publicação do *The Guardian*, Snowden se viu na necessidade de calcular seus passos até a delação, mas de forma a não prejudicar colegas de trabalho, além de ter que pensar em sua própria segurança. Em 2010 ele trabalhava como funcionário terceirizado da Dell para a NSA, o que lhe garantiu acesso privilegiado a informações ultrassecretas. Quanto mais o tempo passava, mais informações perturbadoras chegavam às suas mãos e mais certo da delação ele se tornava. O que se concretizou em 2013 (GREENWALD, 2014).

3.2 WIKILEAKS

É uma organização sem fins lucrativos da Sunshine Press[5], cujo propósito é tornar públicas informações importantes, que podem ser de cunho sigiloso, caracterizando assim seu próprio nome *leak*, que em inglês significa vazamento. Apresenta-se afirmando que proporciona disposição segura e anônima das informações que lhe são enviadas, pois as criptografam. Tais informações são publicadas de forma íntegra, ou seja, não sofrem qualquer tipo de alteração. Sua motivação em divulgar informações que julga de interesse público é apenas de aceitá-las, e não solicitá-las, e baseia-se na Declaração Universal dos Direitos Humanos, mais propriamente o artigo 19, da Declaração, que trata do direito de todos à liberdade de expressão e opinião, além da liberdade de, sem interferência, ter opiniões e de

[5] Sunshine Press é a organização por trás da Wikileaks, é composta por defensores dos direitos humanos, jornalistas consagrados, programadores de *software*, engenheiros de rede, matemáticos entre outros.

procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras. Em alguns casos atrasam a divulgação de alguma informação para proteger a vida e a integridade física de pessoas inocentes (WIKILEAKS, 2007).

A organização também é cercada por advogados à sua disposição que estão comprometidos com os princípios do Wikileaks já que a organização está severamente sujeita a processos de todos os tipos, dada sua missão organizacional.

3.3 EDWARD SNOWDEN EM CONTRAPOSIÇÃO WIKILEAKS

Como a própria palavra **contraposição** significa, esta seção aborda as diferenças e semelhanças entre Edward Snowden e Wikileaks.

Edward Snowden é pessoa física, agiu de acordo com seus princípios morais, mesmo consciente de que sua própria vida pode ser ceifada a qualquer momento a partir da data de divulgação dos documentos confidenciais. Teve de contar com sua inteligência e perspicácia para entrar em contato com Glenn Greenwald, revelar sua história e se proteger de uma possível extradição de Hong Kong (local onde se abrigou), baseando-se nas leis locais (GREENWALD, 2014).

Enquanto isso, a Wikileaks é pessoa jurídica, criada com o fim de divulgar informações que julgam de interesse público, informações essas que lhe são entregues livremente. Como pessoa jurídica, possui um séquito de advogados a defender seus direitos e interesses (WIKILEAKS, 2007).Enfim, o primeiro possuía informações e precisava de um meio de divulgá-las e o segundo recebe informações e as divulga.

Apesar das diferenças, são as semelhanças que fazem Snowden e Wikileaks serem dignos de análise. Ambos são movidos pela ideia de revelar informações que pressupõem afetar a sociedade e que, em seu juízo, devem ser discutidas por esta e assim remover informação privilegiada das mãos de alguns poucos. Afinal, informação gera conhecimento, e conhecimento é poder.

4 COMO OCORRERAM AS DIVULGAÇÕES FEITAS POR EDWARD SNOWDEN

Por seu jornalismo dinâmico e agressivo, Glenn Greenwald foi escolhido, juntamente com Laura Poitras, para tornar públicas as informações em mãos de Edward Snowden. Ambos têm histórico de um jornalismo destemido de ações governamentais em censurar suas reportagens ou artigos que não medem palavras contra o poder público (GREENWALD, 2014).

Após vários contatos e já tendo a posse das informações ultrassecretas, em maio de 2013 os dois jornalistas viajaram à Hong Kong para encontrar seu informante e dar início à entrevista na qual Edward Snowden explica as motivações que o levaram a tomar a decisão que o tornou um prisioneiro sem muros e que abalou as relações de Brasil e Estados Unidos e Alemanha e Estados Unidos. Então no dia 6 de junho de 2013 a matéria foi ao ar na página da Internet do The Guardian, sob o título: “NSA faz coleta diária dos registros telefônicos de milhões de clientes da Verizon”. Como eram muitos arquivos, os jornalistas e Snowden se organizaram de forma a publicar várias matérias em sequência, de maneira que o assunto em si ficasse em foco e não o delator, pois a ideia de Snowden era chamar a atenção para a invasão indiscriminada de privacidade do governo estadunidense sem autorização, tanto para com sua população quanto para com pessoas de interesse de outros países (GREENWALD, 2014). E é claro, as divulgações implicaram em consequências.

4.1 DIVULGAÇÕES

O material foi publicado de forma sistemática, com intervalo de alguns dias entre uma matéria e outra, sendo que 4 dias após a primeira divulgação do The Guardian a identidade de Edward Snowden foi revelada. Sua ideia era que com a revelação tardia de sua identidade, a matéria principal já teria atingido o público e dado tempo suficiente para que todos começassem a digerir o que estava acontecendo, tirando o foco do delator ao mesmo tempo em que impediria que os colegas de Snowden sofressem algum tipo de retaliação por suspeita de envolvimento com a divulgação.

As matérias foram publicadas com início no dia 5 de junho de 2013 ao longo de todo o mês. Neste dia o jornal revelou uma ordem secreta da corte dos Estados

Unidos às maiores companhias de telefonia deste país a fornecer as gravações telefônicas de milhões de seus cidadãos (GREENWALD, 2014).

No dia 6, outra matéria revelou a existência de um programa governamental chamado Prism que obrigou as empresas Google, Facebook, Apple além de outras empresas a fornecerem os dados guardados pelas mesmas.

No dia 7, enquanto Barack Obama, presidente dos Estados Unidos, defendia os dois programas, afirmando que o equilíbrio correto havia sido alcançado, o The Guardian publicou que o *Government Communications Headquarters* (GCHQ, serviço de inteligência britânico), conseguia ver as comunicações de usuários das empresas de Internet dos Estados Unidos justamente porque tinha acesso ao Prism.

No dia 8, outra matéria baseada no vazamento de Snowden revelou a existência de outra ferramenta da NSA chamada *Boundless Informant,* que grava dados e consegue analisar de onde vêm, ao passo que garante ao Congresso dos Estados Unidos, a incapacidade da ferramenta de controlar a vigilância efetuada no país.

No dia 9 é revelada a identidade de Edward Snowden como o responsável pelo vazamento das informações, tal revelação é feita por meio de uma entrevista gravada.

No dia 16, o The Guardian revela que o GCHQ interceptou as comunicações de políticos estrangeiros na cúpula de 2009 do Grupo dos 20 (G20, grupo das 20 maiores economias do mundo: África do Sul, Alemanha, Arábia Saudita, Argentina, Austrália, Brasil, Canadá, China, Coreia do Sul, Estados Unidos, França, Índia, Indonésia, Itália, Japão, México, Reino Unido, Rússia, Turquia e União Europeia).

No dia 20, é publicada a matéria, na qual documentos ultrassecretos revelam como juízes dos Estados Unidos assinaram as ordens que permitiram que a NSA fizesse uso de informações inadvertidamente colhidas de comunicações domésticas de cidadão estadunidenses e, pior ainda, sem mandado judicial.

No dia 21, revelou-se que a GCHQ compartilha com a NSA as informações sensíveis privadas obtidas por intermédio de um acesso ao cabo da rede mundial que carrega chamadas telefônicas e tráfego de Internet.

No dia 1 de julho, Snowden faz um comunicado utilizando-se da página de Internet do Wikileaks dizendo que teve que sair de Hong Kong para preservar sua liberdade e segurança.

Em 8 de julho de 2013, o The Guardian disponibiliza a segunda parte da entrevista com Edward Snowden, na qual ele relata que sabe que o governo dos Estados Unidos irá dizer que ele, Edward, cometeu crimes graves, como violar a lei de espionagem de seu país e que também auxiliou os inimigos fazendo as divulgações sobre o sistema de vigilância da NSA. (GIDDA, The Guardian, 2013). A Lei de Espionagem de 1917 dos Estados Unidos prevê várias sanções, estas tão rigorosas que apresentam entre elas a prisão perpétua e a pena de morte (GREENWALD, 2014).

4.2 CONSEQUÊNCIAS

Como consequência das divulgações, algumas relações diplomáticas foram abaladas, uma vez que em uma das matérias, veio à tona que as comunicações da presidente do Brasil, Dilma Roussef, e da chanceler alemã Angela Merkel estavam sendo monitoradas pelos sistemas da NSA.

Pela falta de resposta do governo estadunidense ao questionamento de Dilma Roussef sobre o monitoramento, a presidente cancelou a viagem que faria aos Estados Unidos na época para encontrar o presidente Barack Obama, ato que demonstrou abalo nas relações entre os dois países aliados.

Já Angela Merkel, que também questionou o monitoramento, manifestou decepção em relação aos Estados Unidos e lançou uma ofensiva diplomática, enviando autoridades de seus serviços secretos para os Estados Unidos. Essa ofensiva teve como objetivo obter explicações sobre a vigilância velada que sofre.

Não se pode dizer que as relações entre os três países se retificaram completamente, ao passo que outros países citados e não citados nos documentos vazados podem ter acionado seus alertas; afinal, agora todos têm certeza do poderio de monitoramento dos Estados Unidos.

Partindo para o cenário atual, ainda se pode ver o resultado de outras divulgações indevidas, como o caso do HSBC. Para tal, o Consórcio Internacional de

Jornalismo Investigativo teve acesso a documentos que revelaram que o HSBC da Suíça foi usado como ponto de lavagem de dinheiro e sonegação de impostos incentivada por funcionários do banco. O escândalo não poupou brasileiros que têm conta na unidade da Suíça que está sendo investigada, ou seja, o problema não está longe nem perto, mas em praticamente todos os lugares. Brasileiros e brasileiras da alta sociedade, empresários e celebridades se veem encurralados a possivelmente prestar esclarecimentos sobre sonegação de impostos. Mais uma vez a quebra de confidencialidade deflagrou um escândalo e o fator humano foi essencial para tal evento.

O delator, Hervé Falciani, diz que o fez por motivos de conduta moral, mas outros veículos informam que ele vendeu as informações, no início de 2008. De acordo com o jornalista Fernando Rodrigues, Hervé e uma ex-colega de trabalho teriam tentado vender dados, inclusive dados confidenciais, a filiais de bancos no Líbano, mas sem informar sua procedência. Tal ação levantou suspeitas dessas filiais, que por sua vez informaram a Associação dos Bancos Suíços da tentativa de venda de dados de clientes. Falciani passou a ser investigado desde então (RODRIGUES, UOL Notícias, 2015). As incertezas sobre sua conduta e versão das autoridades Suíças de que Falciani tentara vender informações contrastam com a conduta de Snowden, que foi categórico do início ao fim sobre suas motivações.

Outro vazamento é sobre a Petrobrás. O super faturamento de obras aliado à compra duvidosa de uma petrolífera dos Estados Unidos são apenas a ponta do *iceberg* da quebra de sigilo de contas bancárias, conversas telefônicas e correio eletrônico, que revelaram um esquema em que retirou bilhões de reais do Brasil e alimentou contas bancárias particulares de donos de empreiteiras e tantos outros envolvidos. A consequência: queda das ações da Petrobrás não só na bolsa de valores de São Paulo, mas na bolsa de Nova Iorque também, além de processos abertos por investidores. Somado a tudo isso, há ainda o aumento da inflação e a ascensão do dólar, a valores nunca antes atingidos desde o plano Real. Em outras palavras, toda essa situação veio à tona pela quebra da confidencialidade.

A investigação teve início em um posto de gasolina, o proprietário do posto, Carlos Habib Chater, tem pendências com a lei há 20 anos por conta de uma casa de câmbio que não tem autorização para funcionar. A partir daí, a polícia federal do Brasil

passou a monitorar as ligações telefônicas de Carlos, que indicavam que ele enviava remessas de dinheiro para o exterior de forma ilegal. Com as investigações, a polícia federal chegou a muitos nomes de políticos, empreiteiros dentre outros e com a adoção da chamada delação premiada, os integrantes do esquema que foram presos passaram a fornecer mais informações sobre a estrutura de lavagem de dinheiro. A motivação para a quebra de confidencialidade se deu por redução das penas a que estão sujeitos os delatores/infratores (FOLHA, 2015).

Ambas as divulgações são fruto de investigações governamentais e que, portanto, tiveram base e autorização legal e judicial para quebra de sigilo. Desta forma, a quebra de sigilo por mandado judicial leva a discussão ao outro lado da questão, quando há a justificativa de que a divulgação de informações confidenciais trará um bem maior e de interesse público, pois neste cenário as consequências acabam, a seu modo, sendo benéficas.

5 PROPOSTAS PARA MITIGAR FALHAS DE SEGURANÇA NO ATRIBUTO CONFIDENCIALIDADE DA INFORMAÇÃO

As falhas de segurança sempre existirão, uma vez que o elo mais fraco é o ser humano (FONTES, 2006). Portanto o que se propõe é a mitigação de falhas, na impossibilidade de extinguí-las permanentemente.

A confidencialidade é um atributo que prevê a proteção da informação contra divulgação indevida e por mais meios tecnológicos, estudos, inovações que se implementem neste campo, o fator humano ainda interfere sobremaneira na manutenção da confidencialidade. Portanto, a proposta deste trabalho é no sentido da adoção de o que se propõe são meios que abordem de forma mais incisiva a questão humana na segurança da informação.

5.1 REVISÕES DAS NORMAS E QUESTÕES DE SEGURANÇA EXISTENTES SOBRE CONTROLES A SEREM FEITOS (AS CAMADAS DE SEGURANÇA – O TRIPÉ CID)

Segundo Edward Snowden para Glenn Greenwald, o primeiro “admite ser possuidor de conhecimentos suficientes para apagar seu rastro nos sistemas da NSA, mas os deixara propositalmente de forma a não envolver os que trabalhavam com ele” (GREENWALD, 2014, p. 60). Ou seja, se há como apagar os rastros, há falhas na segurança, principalmente no que diz respeito à confidencialidade (GREENWALD, 2014).

As práticas mais modernas preveem um leque de opções para a segurança da informação para que confidencialidade, integridade e disponibilidade sejam preservadas. As opções englobam desde a parte de segurança física - como portas que abrem mediante leitura biométrica para locais de acesso restrito – até a parte de segurança lógica, com níveis de permissão de acesso a banco de dados, criptografia, controle de senha e registro de *logs,* entre outros, que permitam que os acessos sejam rastreados, que informem quem teve acesso aos dados, quando e a quais dados (PRADO; SOUZA, 2014, p. 93-105).

A partir destes (e de outros recursos também), a integridade e a disponibilidade das informações podem ser garantidas, mas e quanto à confidencialidade?

Dado o próprio alcance da Internet, a quantidade de informações e ferramentas ali disponibilizadas, é impossível garantir confidencialidade. Pela singularidade de um conjunto de informações que trafegam na Internet é possível determinar seu proprietário, mesmo que de forma indesejável. O processamento de dados digitais, tais como compras, pesquisas sobre algum determinado assunto ou produto, ou mesmo o GPS dos celulares, quando ativos, deixam rastros do dia a dia de um indivíduo. Há cada vez mais ferramentas que possibilitam um infinito de pesquisas, como o projeto Google Flu Trends. Este permite prever um surto de gripe em uma determinada região, medindo-se a quantidade de buscas no Google sobre gripe. Isso mostra que, a quantidade de dados digitais processados proporciona o conhecimento de outra informação, ainda que nenhuma entidade ou órgão tenha notificado a região sobre um surto de gripe (ZALLIS; PENTLAND, Veja 2015, p. 20).

5.2 PROPOSTAS DE MITIGAÇÃO

Dado que o fator humano interfere demasiado na segurança da informação, especialmente no atributo confidencialidade, o investimento no treinamento, conscientização e monitoramento comportamental mostra-se muito relevante. Os vazamentos de informações relatados neste trabalho voltam-se ao ser humano como fonte das revelações. Igualmente, as ferramentas de controle de acesso poderiam ser aperfeiçoadas de forma a notificar o superior imediato do funcionário que acessar, copiar ou fizer tentativas de acesso ou cópia de informações confidenciais, como é feito, por exemplo, com compras suspeitas debitadas em cartão de crédito, no qual o proprietário do cartão é notificado. Ou, em um segundo momento *ex-post-facto*, não permitir que o rastro do acesso seja apagado, como Edward Snowden revelou ser factível (GREENWALD, 2014).

Apesar do investimento em treinamento e conscientização, mostrado na Figura 5, ser de cerca de 25%, pode-se notar que ainda não é o suficiente já que os incidentes de segurança envolvendo pessoas continuam a crescer. Portanto, é necessário que o investimento nessa área seja ainda maior ou que a abordagem para tratar esses incidentes provocados pelo ser humano seja revista, a fim de que os incidentes diminuam. De acordo com Fernando Camarotti, gerente de segurança da informação

da Vale[6], que participou da pesquisa da PwC, no passado, os projetos onerosos inclinavam-se a bloquear os dados mas que agora não são vistos mais como eficazes e que atualmente, eles trabalham para encontrar quais informações confidenciais precisam ser protegidas, tornando assim o investimento em segurança mais inteligente e efetivo.

Outra proposta que se mostra válida, mas que depende do governo federal e que, portanto, é uma proposta que talvez possa provocar um prazo mais longo para ser resolvida, é a melhoria na regulamentação da legislação que abrange os crimes que envolvem a segurança da informação. Apesar da lei 12.965 (também conhecida como Marco Civil da Internet) ter sido sancionada em 23 abril de 2014, há ainda muitos desafios no campo jurídico, envolvendo os crimes cibernéticos. Como adiantou Gonçalves em seu artigo de 4 abril de 2003 “Este é o maior desafio jurídico que a rede nos apresenta para ser resolvido e que, ao que parece, continuará por um bom tempo sem resposta”. Mais de 10 anos se passaram e seu artigo continua atual, pois o Brasil está no início da regulamentação de leis sobre tais crimes, visto que algumas leis, como a 12.737 de 30 de novembro de 2012, foi sancionada após o furto e divulgação indevida de fotos íntimas da atriz brasileira Carolina Dieckman, ou seja, a lei surge depois do delito quando poderia antecipar-se a ele.

Outro ponto importante é a vigilância, não apenas sobre as pessoas comuns, mas também sobre o governo como um todo. Uma publicação do jornal O Estado de São Paulo (8 de maio de 2015) informou que os grampos praticados pela NSA foram considerados ilegais pela justiça dos Estados Unidos; ora, sendo a NSA um órgão governamental deste país, não deveria este estar acima de qualquer suspeita? Isto coloca em xeque a legitimidade do governo perante a ilegitimidade de Snowden de trazer à tona informações confidenciais. De um lado o governo estadunidense acusa Edward de violar a Lei de Espionagem, do outro, o governo se vê agora como réu, já que as escutas realizadas foram consideradas ilegais. Em 16 de maio, o mesmo jornal informa que a Petrobrás “admitiu ser vulnerável à espionagem” e que, segundo os técnicos da estatal, seria impossível garantir sigilo frente à NSA, porque a agência estadunidense possui sistema muito avançado que pode furar qualquer tipo de

[6] Vale é uma empresa brasileira de mineração.

segurança. Esta notícia coloca novamente em xeque a legitimidade da NSA em espionar os países considerados aliados.

A sociedade precisa estar atenta às ações do governo e reivindicar, no mínimo, clareza na gestão do país, por mais difícil que pareça de se conseguir (O ESTADO DE SÃO PAULO, 2015).

6 CONSIDERAÇÕES FINAIS

O **problema** apresentado pelo trabalho foi a divulgação de informações sigilosas por pessoas em cargos de confiança que podem causar impacto danoso ou gerar sérias crises e a **pergunta** associada ao problema foi: há maneiras de minimizar a divulgação de informações sigilosas que podem causar graves crise?

Os fatos divulgados por Snowden causaram crise diplomática, como visto no Capítulo 4, seção 4.2, além de abrir as portas para incidentes de segurança semelhantes, como ocorrido com o HSBC, visto também Capítulo 4, seção 4.2 e Operação Lava Jato, entre outros, que atingem seriamente pessoas e organizações de diversos países. Portanto, a quebra da confidencialidade mostra-se altamente danosa.

A **hipótese (a)**, que trata do treinamento exaustivo, foi reforçada pelos resultados da PwC, Figura 5, indicando o aumento de investimento no recurso humano.

A **hipótese (d)**, que trata da necessidade de outros recursos associados à segurança, confirmou-se através da entrevista do co-fundador do Instituto de tecnologia de Massachusetts (MIT) à revista Veja, em 11 de março de 2015. Nesta entrevista o cientista Pentland afirma que não se pode mais garantir a confidencialidade, no que diz respeito à segurança das informações que trafegam na Internet. Ele destaca que escreveu um livro, no qual prova (usando conceitos matemáticos) esta afirmação. A autora pesquisou o sobre o livro, mas até a conclusão deste trabalho o livro ainda não chegou ao Brasil.

O objetivo geral e os objetivos específicos deste trabalho foram atingidos, conforme conteúdos dos Capítulos 3, 4 e 5, suas seções e subseções.

Sugestões para trabalhos futuros apontam na direção de se repensar sobre o tripé de segurança da informação – confidencialidade, integridade e disponibilidade. Isto significa pesquisas sobre novas ferramentas associadas à segurança, mudança na abordagem de tratamento da questão confidencialidade (pelo menos), mudança na legislação vigente e mudança de postura no controle de ações de colaboradores

de organizações. Lembrando Pentland: “é algoritmicamente impossível analisar dados pessoais sem identificar de onde vêm” (Revista Veja, 2015, p. 21).

A advogada Patrícia Peck Pinheiro, autora do livro Direito Digital, propõe que as leis já exitentes sejam aplicadas aos crimes digitais pela semelhança do delito praticado, como por exemplo, o estelionato. Este é previsto no artigo 171 do código penal e poderia ser aplicado no caso de *Phising Scan,* que constitui de induzir o usuário a acessar um *e-mail* falso e este, contendo um código malicioso que quando executado, furta informações do usuário e as transporta para o fraudador (PINHEIRO, 2010, p. 310-316).

A vastidão de dados e tecnologia disponíveis na Internet trazem à tona o personagem principal do livro de Dostoiévski, Crime e Castigo. Neste, um desafortunado jovem estudante de direito, publica em um jornal da cidade, um artigo em que defende existir, no mundo, dois tipos de pessoas: as ordinárias e as extraordinárias. As ordinárias são as pessoas comuns que formam a grande massa da sociedade enquanto que as pessoas extraordinárias nascem uma a cada geração, com o fim de promover o adiantamento da humanidade, mesmo que para isso tenham que cometer uma contravenção. O personagem então se vê em conflito com suas convicções por ter cometido assassinato, que a seu ver traria um bem comum para a sociedade já que sua vítima era uma agiota. Mas em seu íntimo, não consegue conviver com seu crime e vive atormentado pela culpa, evidenciando que ele não faz parte das pessoas extraordinárias (DOSTOIÉVSKI, 2007).

A conclusão da autora, acrescida a este paralelo à obra de Dostoiévski, é de que cada vez mais, pessoas como Edward Snowden e entidades como Wikileaks podem surgir, agir e assim trazer reflexões sobre crime e castigo e os dois lados da moeda.

REFERÊNCIAS

ALEVATE, William. **Gestão da Continuidade de Negócios.** 1ª. ed**.** Rio de Janeiro : Elsevier, 2014.

BBC News. Edward Snowden: Timeline. **BBC News**, US & Canada, 20 agosto 2013. Disponível em: <http://www.bbc.com/news/world-us-canada-23768248>. Acesso em 9 nov. 2014.

BRASIL. Lei no. 12.965, de 23 de abril de 2014. **Planalto**, Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, Brasília, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 24 mai. 2015, às 15h58min.

BRASIL. Lei no. 12.737, de 30 de novembro de 2012. **Planalto,** Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, Brasília, 30 nov. 2012. Disponível em:
<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em 24 mai. 2015, às 15h59min.

CLARY, Timothy A. Guardian revela identidade de fonte de vazamentos sobre inteligência dos EUA. **Exame.com**, São Paulo/SP, 9 junho 2013. Disponível em: <http://exame.abril.com.br/mundo/noticias/guardian-revela-identidade-de-fonte-de-vazamentos-sobre-inteligencia-dos-eua>. Acesso em 9 nov. 2014.

DOSTOIÉVSKI, Fiódor. **Crime e castigo**. Trad. Ivan Petrovich, Irina Wisnik Ribeiro. São Paulo : Martin Claret, 2007. 555p.

FABRINI, Fábio. Petrobrás admitiu ser vulnerável à espionagem. **O Estado de São Paulo**, São Paulo/SP, p. B5, 16 maio 2015. (Economia)

FOLHA de São Paulo. Sucursal de São Paulo. Entenda a operação lava jato, da Polícia Federal. **Folha de São Paulo**, São Paulo, 14 de novembro de 2014 (conteúdo atualizado em 06 de junho de 2015).
Disponível em: <http://www1.folha.uol.com.br/poder/2014/11/1548828-posto-de-gasolina-no-df-motivou-operacao.shtml>. Acesso em: 30 jun. 2015, às 21h31min.

FONTES, Edison L. G. **Praticando a segurança da informação**. 1ª. ed. Rio de Janeiro: Brasport, 2006.

FRANCE Presse. Alemanha lança ofensiva diplomática após espionagem da NSA a Merkel. **Correio Braziliense**, Brasília/DF, 26 outubro 2013. Disponível em: < http://www.correiobraziliense.com.br/app/noticia/mundo/2013/10/26/interna_mundo,395568/alemanha-lanca-ofensiva-diplomatica-apos-espionagem-da-nsa-a-merkel.shtml>. Acesso em 16 mar. 2015, às 21h32min.

GASETA, Edson Roberto. **Princípios de Segurança da Informação**. Americana: Faculdade de Tecnologia de Americana, 2012. 50 slides, color., 10cm x 5cm (Materiais didáticos instrumentalizados na disciplina de "Princípios de Segurança da Informação", alocada no 1º semestre do Curso Superior de Tecnologia em Segurança da Informação).

GIDDA, Mirren. Edward Snowden and the NSA files – timeline. **The Guardian,** New York/NY, 21 agosto 2013.
Disponível em: <http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>. Acesso em: 16 mar. 2015.

GONÇALVES, Sérgio Ricardo M. Hackers, Crackers e Spammers: quem são e o que fazem? **Mundo jurídico**. Disponível em <www.mundojuridico.adv.br>. Acesso em: 4 mai. 2003.

GRADILONE, Cláudio. A lavanderia suíça do HSBC. **Isto é dinheiro**, 13 fevereiro 2015. Disponível em:
<http://www.istoedinheiro.com.br/noticias/financas/20150213/lavanderia-suica-hsbc/232989.shtml>. Acesso em 28 mai. 2015, às 15h44min.

GREENWALD, Glenn. **Sem lugar para se esconder**. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

GREENWALD, Glenn; POITRAS, Laura. NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video. **The Guardian,** New York/NY, 9 junho 2013. Disponível em:
<http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>. Acesso em: 9 nov. 2014.

Information Security Survey. **PwC**.
Disponível em: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml>. Acesso em 22 abr. 2015

KUROSE, James Francis; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. Trad. Opportunity translations. 5ª. ed. São Paulo: Pearson, 2010.

MARQUES, Julia. NET demite funcionário por assédio online. **O Estado de São Paulo**, São Paulo/SP, p. A15, 16 maio 2015. (Metrópole)

MPE exportação 2011 Brasil. **SEBRAE**. Disponível em: <www.sebrae.com.br/Sebrae/Portal%20Sebrae/Estudos%20e%20Pesquisas/MPE%20exportacao%202011_Brasil.pdf>. Acesso em: 18 mai. 2015.

Pesquisa Global de Segurança da Informação 2014. **PwC**. Disponível em: http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/pesquisa-global-seguranca-informacao-14.jhtml. Acesso em: 22 abr. 2015.

PINHEIRO, Patricia Peck. **Direito Digital**. 4ª. ed. rev., atual. e ampl. São Paulo : Saraiva, 2010 (p. 71-77, 310-316).

PRADO, Edmir P. V.; SOUZA (ORG), Cesar Alexandre de (ORG). **Fundamentos de sistemas de informação.** 1ª ed. Rio de Janeiro : Elsevier, 2014 (p. 55-76, 93-110).(15 capítulos divididos em 4 partes: Primeira parte com 4; segunda com 5; terceira com 3; e quarta com 3 capítulos)

REOLOM, Mônica. Registros de crime virtual em cartório crescem 88% no país em dois anos. **O Estado de São Paulo**, São Paulo/SP, p. E1, 16 maio 2015. (Metrópole)

RODRIGUES, Fernando. Denunciante? Ladrão? Herói? A fonte dos dados que balançaram o HSBC. **Blogosfera Uol**, 8 fev. 2015. Disponível em: <http://fernandorodrigues.blogosfera.uol.com.br/2015/02/08/denunciante-ladrao-heroi-a-fonte-dos-dados-que-balancaram-o-hsbc/>. Acesso em: 31 mai. 2015, às 21h28min.

TREVISAN, Claudia. Tribunal diz que grampos da NSA são ilegais. **O Estado de São Paulo**, São Paulo/SP, p. A10, 8 mai. 2015. (Internacional)

Vale. Sobre. **Vale**.
Disponível em: < http://www.vale.com/PT/aboutvale/Paginas/default.aspx>. Acesso em: 19 mai. 2015.

VALENTE, Rubens. Posto de gasolina no DF motivou operação. **Folha de São Paulo**, Brasília/DF, 16 novembro 2014. Disponível em: <http://www1.folha.uol.com.br/poder/2014/11/1548828-posto-de-gasolina-no-df-motivou-operacao.shtml>. Acesso em: 28 mai. 2015, às 15h50min.

Wikileaks. Sobre. **Wikileaks**. Disponível em: <https://wikileaks.org/>. Acesso em: 9 mar. 2015.

ZALLIS, Pieter. Entrevista: Alex Pentland. **Revista Veja**, São Paulo, ano 48, nº 10, Edição 2416, p. 17-21, 11 de março de 2015.