Terêncio
ISSN: XXXX-XXXX

SEGURANÇA DE INFORMAÇÕES INDUSTRIAIS, ESPIONAGEM INDUSTRIAL E VAZAMENTO DE PROJETOS

Entrevista com o Prof. João José de Souza

Heitor Mozelli Bezerra
Maurício Hideyuki Tomita
Raul Alves Picasso
Artur de Lima Dalmasso
Curso de Engenharia
Centro Universitário FEI

Palavras-chave: espionagem industrial, vazamento de informações sigilosas, políticas de compliance industrial

O entrevistado, **João José de Souza,** possui graduação em Engenharia Industrial pela Universidade Santa Cecília (1990), Mestrado em Engenharia de Energia pela Universidade Federal de Itajubá (2006), Especialização em Administração de Empresas pela Fundação Getúlio Vargas (2003) e Especialização em Docência em Ambientes Virtuais e Neurociências pela PUC del Equador. Atualmente é professor adjunto da Universidade Santa Cecília e no Centro Universitário da FEI. Possui experiência na área de Engenharia Mecânica, com ênfase em Projetos de componentes, processos de fabricação, elementos de máquinas e qualidade assegurada. Possui experiência internacional, tendo realizado visitas técnicas (Alemanha e Rep. Tcheca), cursos (Argentina), Conferências (Alemanha, Espanha e Polônia) e auditorias (Argentina, Colômbia, Venezuela e Estados Unidos). Foi membro da Comissão da Qualidade da ANFAVEA (2016 - 2021) representando a Volkswagen do Brasil. Membro do Comitê Técnico da Qualidade do IQA - Instituto da Qualidade Automotiva(2021).

Da época em que o Sr. se formou até hoje, onde avalia que as empresas vêm mais investindo na proteção de seus projetos?

Proteção de projetos e informações é algo muito crítico na indústria, muita gente não tem ideia do tamanho da preocupação. Imagine que você

vai desenvolver um produto, um processo novo: isso requer um investimento forte, às vezes se investe alguns milhões, há casos em que são investidos bilhões de dólares ou euros. Então se essas informações vazam, o prejuízo pode ser muito grande, porque o concorrente pode se aproveitar dessas informações para sair na frente.

Imagem 1: Professor João José de Souza

Fonte: http://lattes.cnpq.br/1624402095512504

Se alguém está desenvolvendo algo inovador, a intenção é sair na frente do mercado, seja criando um mercado novo ou mudando o atual, e consequentemente conquistar uma grande fatia e faturar mais. Se essa informação vaza, o que acontece? Perde-se vantagem competitiva, esse é o grande problema e por isso se vem investindo cada vez mais na proteção de dados. Hoje em dia, preza-se muito pelo sigilo na telefonia; existem certas coisas que não se deve discutir por telefone. Computadores que possuem acesso a sistemas de servidores tornaram o uso de "firewall" essencial para a segurança cibernética das indústrias, ainda mais depois da pandemia, pois a necessidade do acesso remoto por VPN fez o uso de laptop (notebook) crescer muito, ou seja, é preciso ter um sistema de criptografia para garantir que quem está entrando ali é somente o funcionário. Para se ter noção, na Volkswagen existem sistemas cuja senhas de acesso mudavam a cada 60 segundos e só era possível o acesso por meio de um aparelho que era sincronizado com a mudança para garantir o sigilo.

Quando se tem projetos de montadoras, em que o carro entra em fase de teste, não se permite a entrada de celular onde o projeto está sendo desenvolvido. Se é necessário entrar, a segurança do local coloca um selo no celular e, caso haja violação do selo, com certeza as consequências serão apenas questão de tempo. Algumas vezes a segurança pede para a pessoa desbloquear o celular, anota o ID do aparelho, o nome da pessoa, o registro de funcionário. Se por acaso vazar uma foto gerada nesse aparelho, eles têm pleno conhecimento de quem vazou.

Fora isso, existe pessoal especializado na captura dessas informações, é questão de sobrevivência investir na proteção de informações sigilosas.

ISSN: XXXX-XXXX

Seria mais o setor bélico que tem esse pessoal especializado?

Não, aí é que você se engana. O ramo farmacêutico é muito priorizado, automobilístico também, pois é possível perder grandes vantagens em função de um produto ou serviço que outros não possuem. Projetos novos, como carros elétricos e os híbridos, envolvem muito dinheiro. Se essa informação é perdida, isso representa um problema.

O que acha do atual estado da indústria (dentre nacionais ou multinacionais que estão inseridas no Brasil) com relação à segurança?

É perceptível que estão investindo cada vez mais em segurança, eles costumam investir além da parte de informática. As empresas têm muito treinamento, por exemplo contra corrupção (não necessariamente o sujeito recebe dinheiro para superfaturar algo em benefício próprio, mas sim vender informação), código de conduta etc. A Volkswagen por exemplo tem esse treinamento e os funcionários têm quem renová-lo todo ano. É obrigatório, as pessoas respondem *online* e ainda recebem um certificado. Depois, segue uma lista para a diretoria de quem respondeu, e a diretoria ainda vai cobrar os gerentes do porquê algum funcionário não renovou. O índice de respostas é obrigatoriamente 100%.

Hoje, também, as empresas estão implementando uma nova norma internacional, a ISO 27001, que estabelece um sistema de gestão de segurança da informação, que ajuda a padronizar processos e aumenta a confiança dos *stakeholders* nas empresas. Além das normas, no Brasil temos a LGPD, a Lei Geral de Proteção de Dados, com a função de proteger dados pessoais. Na fábrica mesmo, às vezes alguém ligava pedindo o telefone de outra pessoa e, conforme a LGPD, é dado sensível; então eu mandava um e-mail dizendo quem queria entrar em contato. Muitas dessas empresas também já implementaram gerenciamento de risco e *compliance*. Existem grandes gerências dentro das empresas para verificar se há a existência de conflitos que comprometem o sigilo de informações importantes. Existem auditorias internas que investigam se tem gente fazendo coisa errada e finalmente tem o *compliance* e gerenciamento de risco, que investigam riscos que possam circundar setores como a parte financeira.

O Sr. poderia dar um exemplo de um vazamento grande que ocorreu? Este caso seria possível combater ou apenas minimizar os danos?

Separei dois casos que são públicos; inclusive um deles aconteceu enquanto eu já estava no mercado.

Não são confidenciais, deixando claro que são de conhecimento da imprensa. O primeiro caso é famoso: o ex-executivo da GM, José Ignacio López de Arriortúa, que em 1993 foi para a Volkswagen. A GM na época estava desenvolvendo um novo conceito de fábrica, de como a fábrica iria operar, e quando esse executivo foi para a Volkswagen, a própria VW implementou isso aqui no Brasil. Esse conceito está em operação hoje na fábrica modular de caminhões e ônibus de Resende, no Rio de Janeiro. Basicamente, a modularidade consiste em dar ao fornecedor a responsabilidade das operações e o fornecedor é pago assim que o veículo recebe o *ok* e liberação: é assim que a fábrica de Resende funciona. No total, são poucos os funcionários da Volkswagen, são praticamente de engenharia e qualidade, o restante é os fornecedores. Na montagem de um caminhão, por exemplo, na prática quem monta dentro da fábrica não é um funcionário da VW, mas sim o fornecedor responsável por tal operação. O fornecedor só recebe o faturamento quando o caminhão já está no pátio esperando a venda. Contabilizado esse veículo, o pagamento é feito. Isso foi revolucionário, dizem que na época a GM já tinha esse plano e de repente a VW aparece com essa ideia, e justamente quem comandava a fábrica era esse ex-executivo.

Imagem 2: José Ignacio López de Arriortúa.

Fonte: https://www1.wdr.de/stichtag/stichtag-beginn-lopez-affaere-100.html

Após uma guerra de 4 anos na justiça dos EUA, a Volkswagen aceitou pagar uma indenização de 100 milhões de dólares à GM e ainda gastar 1 bilhão na compra de peças da concorrente. Conclui-se que o vazamento de

informações não ataca somente produtos, ataca também a integridade de conceitos de grande porte.

O segundo caso ocorreu quando eu já estava na fábrica da VW, foi o vazamento do Virtus. Em 2017 tinha sido lançado o Polo, um funcionário tirou fotos do carro ainda dentro da fábrica.

Imagem 3: Foto vazada do VW Virtus dentro da fábrica

Fonte: https://www.car.blog.br/2017/08/vazamento-do-virtus-apenas-um.html

Neste caso o funcionário que tirou as fotos foi pego facilmente, pois ele tirou de uma posição que, quem conhece a fábrica, sabia exatamente o local em que a foto foi feita. Quando eu vi as fotos eu já sabia até que em que ala que fotografaram. Essa foto entregou o funcionário por causa da esteira, quem conhece a linha de montagem da VW sabe que essa ala era a 14.

Em que momento uma empresa ou um funcionário de uma equipe deve desconfiar da espionagem?

Sempre. Por isso, existem os treinamentos anticorrupção e de código de conduta. Todo funcionário deve sempre estar em dia nesses treinamentos. Porque conhecendo a conduta correta dentro da empresa, fica mais fácil de reconhecer hábitos fora do padrão estabelecido. O treinamento ensina como lidar com isso. Na VW, caso alguém visse algo estranho, era possível fazer a denúncia para o setor de *compliance*, para a auditoria e, dependendo do nível, era possível denunciar para esses setores na sede alemã. Existem canais diretos que efetuam essa comunicação. Justamente, com esses canais é quase impossível que quem vaze algo sem sair despercebido, pois o contra-ataque vem do alto escalão.

ISSN: XXXX-XXXX

O Sr. já presenciou alguma situação semelhante enquanto membro da ANFAVEA e/ou IQA?

Não, enquanto eu estava na comissão de qualidade na ANFAVEA e do IQA não. Inclusive, quando desenvolvíamos algum trabalho na comissão de qualidade, na ANFAVEA por exemplo (que tem representantes de várias empresas), quando surgia um tema em discussão até para se ter essa discussão era difícil, pois existia um receio entre as empresas de que alguma informação que pudesse expor algo sigiloso. Por exemplo: se alguém compra um carro zero, as montadoras pagam uma empresa para fazer a pesquisa de satisfação, com 3 meses ou 1 ano de uso, e essas informações vão apenas para as montadoras participantes. Quem é de fora não deve receber essas informações, inclusive as montadoras devem ter cautela, pois não é permitida a criação de propagandas utilizando esses dados. As empresas assinam um termo quando entram na associação se comprometendo a não vazar esse tipo de dado. Quando eu estava lá dentro, tinha acesso às informações, sabia o que dava de problema em carro da Fiat, da Toyota etc. e, pelo fato de ser uma associação bem limitada, caso houvesse um vazamento, era fácil descobrir o responsável. Para se ter ideia, quando os resultados das pesquisas eram apresentados e compilados, não era distribuído o material para qualquer setor, somente diretores-presidentes e gerentes de alto escalão tinham acesso. E como não se podia divulgar isso para qualquer um, nos documentos tinha uma marca d'água com o nome do pessoal que recebia e essas informações.

O Sr. considera que esse assunto é devidamente abordado no ambiente universitário?

Não, porque na universidade infelizmente não temos espaço para tratar de tudo que se necessita na formação do profissional. O grande problema é que temos uma grade curricular e tempo limitado para formação dos estudantes. Se nós passarmos tudo que é necessário, o curso será extremamente extenso. Fora isso, se formos adicionar todas as coisas novas na grade, será necessário renovar praticamente todo ano. Eu acredito que esse assunto não é abordado da maneira que deveria ser. Uma grande reclamação que eu ouvia na comissão era que os engenheiros recém-formados não conhecem qualidade, não têm formação, as empresas têm que treinar esses engenheiros em qualidade.

ISSN: XXXX-XXXX

Existir um treinamento específico para cada empresa não adianta?

Não é isso, os recém formados não conhecem nem os conceitos básicos, isso no Brasil inteiro. Hoje já está entrando tanta coisa nos currículos que as faculdades não conseguem espaço para alocar esses requisitos na grade, se não realmente o curso iria ter uns 15 anos. Esses requisitos são cobertos na pós-graduação, onde a pessoa já chega com sua formação básica de engenheiro e se especializa em determinada área. Assim como um médico, que pode ser clínico geral e os especialistas. Esse fenômeno em si não é uma falha, mas uma consequência da quantidade tremenda de novidades que não conseguem ser comportadas pela grade curricular.

É por isso que, quando entra em uma empresa, o profissional já empregado passa por um processo de integração, que consiste em uma apresentação das políticas da empresa. Após isso, ele é treinado dentro do seu setor com os conhecimentos específicos que precisa possuir. Então o gestor da área analisa a equipe para saber quais os recursos e quem receberá esses recursos dentro da equipe. É um processo verdadeiramente meticuloso a inserção desse engenheiro dentro de uma equipe, pois existe bastante dinheiro aplicado, a empresa não pode se dar ao luxo de pagar um curso para alguém que não precisa, para depois enfrentar as consequências de um erro cometido por um membro da equipe mal treinado.

Nessa integração, a primeira coisa é segurança do trabalho, depois vem o código de conduta, o treinamento anticorrupção, as políticas da empresa, e após isso vêm os treinamentos mais específicos de cada membro.

Para um aluno que queira se informar sobre isso, onde o Sr. recomenda pesquisar?

Pode-se começar pelas novas normas, como a ISO 27001 e a ISO 9001 que tem foco no gerenciamento de risco e qualidade e *compliance*.