What executives need to know about cybersecurity

Stuart Madnick

Working Paper CISL# 2019-17

June 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

What executives need to know about cybersecurity

C6 Bank Follow
Jun 10 · 4 min read

For Stuart Madnick, a C6 Bank technology council member, when it comes to cybersecurity, CEOs have to take as their starting point a basic question: "What is the priority of my organization?"

Stuart Madnick, MIT professor and member of the technology council of C6 Bank

Stuart Madnick understands cybersecurity as few. Author and co-author of more than 300 articles and books (beginning with *Computer Security* , 1979), he tracks the evolution of computer security from the pre-internet world. Today, its focus is on how companies - including C6 Bank - view cyber security in their everyday lives.

Além de professor de tecnologias da informação na MIT Sloan School, a escola de negócios do Instituto Massachusetts de Tecnologia (MIT), Madnick comanda um grupo de pesquisa que estuda melhorias na cibersegurança de infraestruturas críticas (sistemas essenciais para o fornecimento de serviços à sociedade, como energia, telefonia e serviços financeiros). As pesquisas ocorrem em parceria com uma série

de empresas e instituições de reconhecimento mundial, como Nasdaq, IBM e Swift. O C6 Bank faz parte desse grupo desde 2018.

Madnick, que também **é um dos membros do conselho de tecnologia do C6 Bank**, esteve recentemente na nossa sede, em São Paulo, para uma série de bate-papos sobre cibersegurança. O modo como as companhias entendem a segurança cibernética, do nível técnico ao executivo, e o controle de processos foram alguns dos principais tópicos abordados pelo professor. Veja, abaixo, algumas de suas ideias.

Como pensar a cibersegurança de uma forma holística

Ninguém espera que o principal executivo de sua empresa escreva códigos criptografados, certo? A não ser que ele seja formado em ciência da computação ou um autodidata na área, é natural que administradores não dominem o mundo da programação. E tudo bem, segundo Madnick.

"Espera-se, no entanto, que o executivo do topo decida o quanto de dinheiro ele vai dedicar à cibersegurança, como funcionarão os níveis de reporte dentro da companhia (quem reporta para quem) e quais as prioridades", diz o professor.

Não adianta, da mesma forma, pensar na cibersegurança apenas da porta para fora. Criar uma cultura interna de cibersegurança, na avaliação de Madnick, é crucial. Entre 70% e 80% dos ataques ocorridos nas companhias são facilitados (em sua maior parte, de forma não intencional) por pessoas de dentro da própria companhia, segundo estimativas de mercado.

Madnick conta que, para ensinar a importância da identificação de riscos às empresas, ele e sua equipe se inspiraram em um método criado por um pesquisador do MIT para prevenir acidentes aéreos. A técnica contém dois pontos-chave:

Definição das prioridades da empresa—O que realmente é importante para a companhia? O que o CEO definiu como prioridade? "Parecem questões simples, mas é muito difícil para a maior parte dos executivos, porque eles nunca foram treinados para pensar nisso", diz Madnick. "É preciso concentrar a energia nas coisas que você mais precisa proteger." No caso da companhia aérea, a prioridade, lembra o professor, é que a aeronave não caia.

Controle de processos—"As pessoas não pensam nisso, mas tudo que acontece na sua organização é um processo", afirma Madnick. "E todo processo tem uma forma de monitoramento e controle. Os processos podem ser eletrônicos ou humanos, mas todos têm uma forma de controle." A pergunta a ser feita, nesse caso, é: como têm funcionado esses controles?

Alguns dos eventos cibernéticos mais conhecidos envolveram falha em um ou nos dois pontos acima, segundo o professor.

Além desses dois pontos-chave, há uma série de medidas que podem ser tomadas para garantir a segurança na prestação de serviços tecnológicos, como testes internos de software e auditorias conduzidas por consultorias externas e internas. Outra opção é testar as aplicações junto a uma comunidade grande de pesquisadores de segurança, como ocorre nos **programas de bug bounty**, por exemplo.

A implementação de serviços online e móveis, como sabemos, é um caminho sem volta. O segmento financeiro não escapa. No Brasil, 60% das transações bancárias já são feitas pelos canais digitais (celular ou computador), segundo a Pesquisa Febraban de Tecnologia Bancária 2019. O segredo para enfrentar esse desafio, segundo Stuart Madnick, é maximizar os benefícios e reduzir os riscos o máximo possível.

Por que o C6 Bank tem um conselho de tecnologia

O C6 Bank criou um conselho de tecnologia em 2018. Ele é composto por três professores do MIT que nos orientam nos assuntos relacionados a novas tecnologias. Entendemos que ter acesso a acadêmicos de uma das instituições mais reconhecidas no mundo é **essencial para quem quer estar à frente no mercado.**

"Mas o que eles ensinam a vocês?", você deve estar pensando. Ainda não podemos revelar os detalhes dos produtos e serviços que estamos criando. Afinal, ainda nem lançamos o banco (o que está previsto para os próximos meses). Mas as interações com os professores do MIT, que ocorre semanalmente, têm nos **ajudado, e muito, na criação e no aperfeiçoamento de soluções que serão úteis no dia a dia do cliente.**

Ah, mais um detalhe sobre Stuart Madnick, a nossa interlocução no MIT para assuntos de cibersegurança: além de também atuar como

professor na escola de engenharia do MIT, ele é membro do Grupo de Tecnologia da Informação da MIT Sloan, papel que tem exercido nos últimos 40 anos (em duas dessas quatro décadas, aliás, Madnick foi o chefe do grupo). Fera, né?