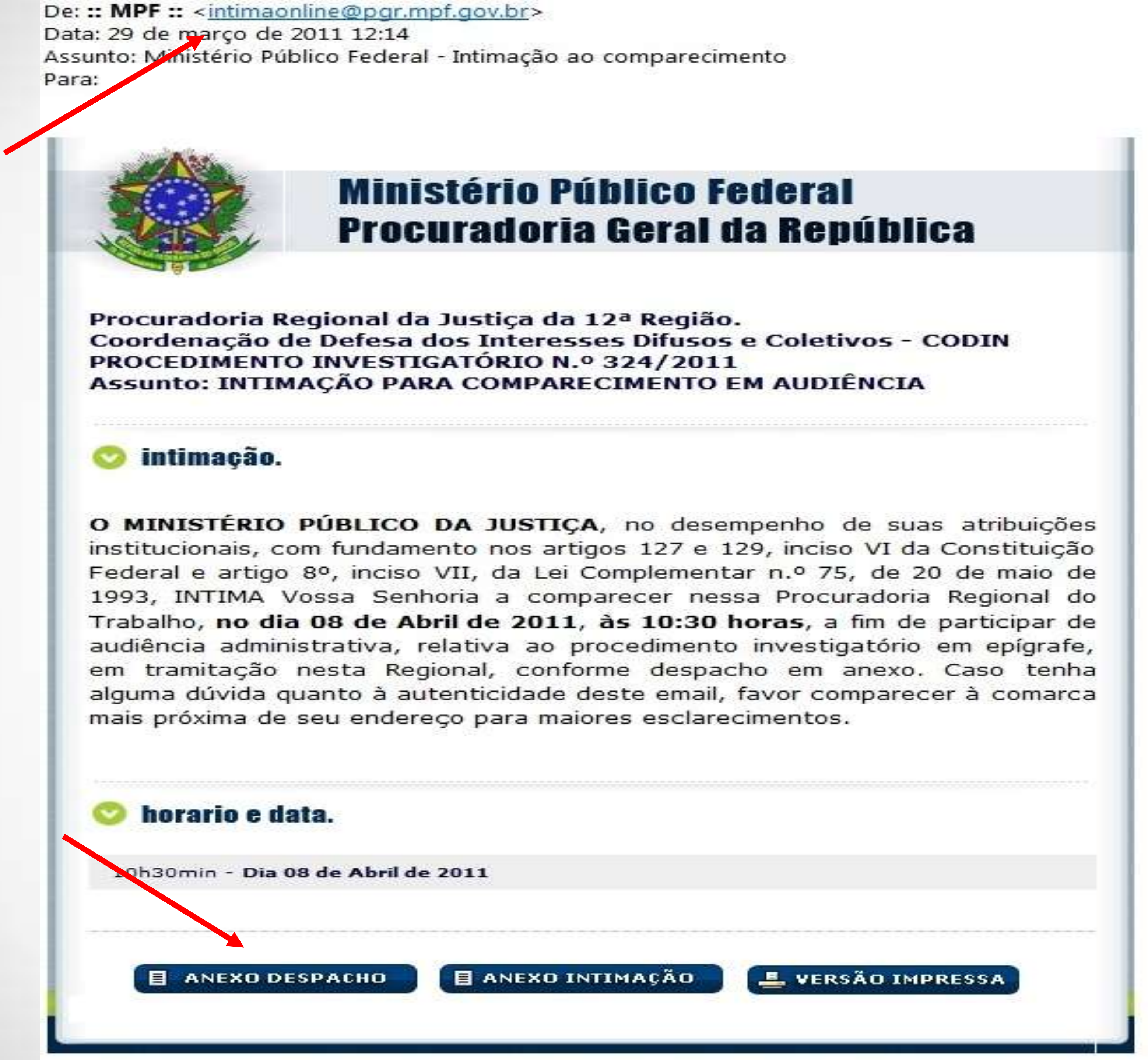
Perícia Forense

OBSTÁCULOS E DESAFIOS

Marcelo Caiado, M.Sc, CISSP, GCFA, EnCE, GCIH
Chefe da Divisão de Segurança da Informação / PGR



De: :: **MPF** :: <intimaonline@pgr.mpf.gov.br>
Data: 29 de março de 2011 12:14
Assunto: Ministério Público Federal - Intimação ao comparecimento
Para:

Ministério Público Federal
Procuradoria Geral da República

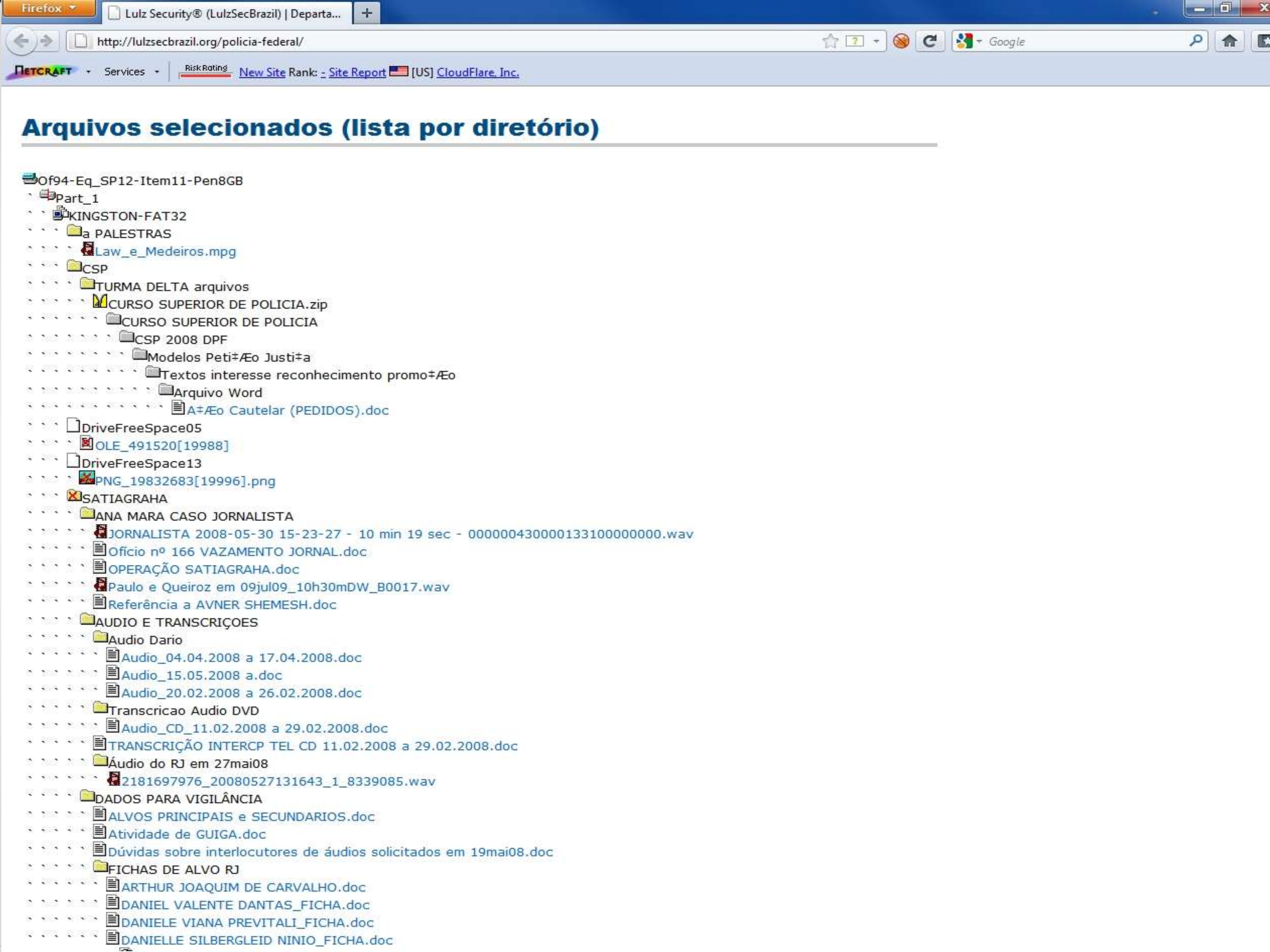
Procuradoria Regional da Justiça da 12ª Região.
Coordenação de Defesa dos Interesses Difusos e Coletivos - CODIN
PROCEDIMENTO INVESTIGATÓRIO N.º 324/2011
Assunto: INTIMAÇÃO PARA COMPARECIMENTO EM AUDIÊNCIA

intimação.

O MINISTÉRIO PÚBLICO DA JUSTIÇA, no desempenho de suas atribuições institucionais, com fundamento nos artigos 127 e 129, inciso VI da Constituição Federal e artigo 8º, inciso VII, da Lei Complementar n.º 75, de 20 de maio de 1993, INTIMA Vossa Senhoria a comparecer nessa Procuradoria Regional do Trabalho, **no dia 08 de Abril de 2011, às 10:30 horas**, a fim de participar de audiência administrativa, relativa ao procedimento investigatório em epígrafe, em tramitação nesta Regional, conforme despacho em anexo. Caso tenha alguma dúvida quanto à autenticidade deste email, favor comparecer à comarca mais próxima de seu endereço para maiores esclarecimentos.

horario e data.

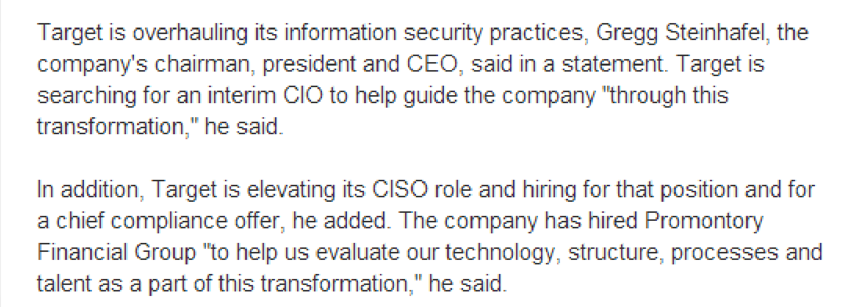
10h30min - **Dia 08 de Abril de 2011**


Firefox
Lulz Security® (LulzSecBrazil) | Departa...
http://lulzsecbrazil.org/policia-federal/
Google
NETCRAFT
Services
Risk Rating
New Site Rank: - Site Report [US] CloudFlare, Inc.

Arquivos selecionados (lista por diretório)

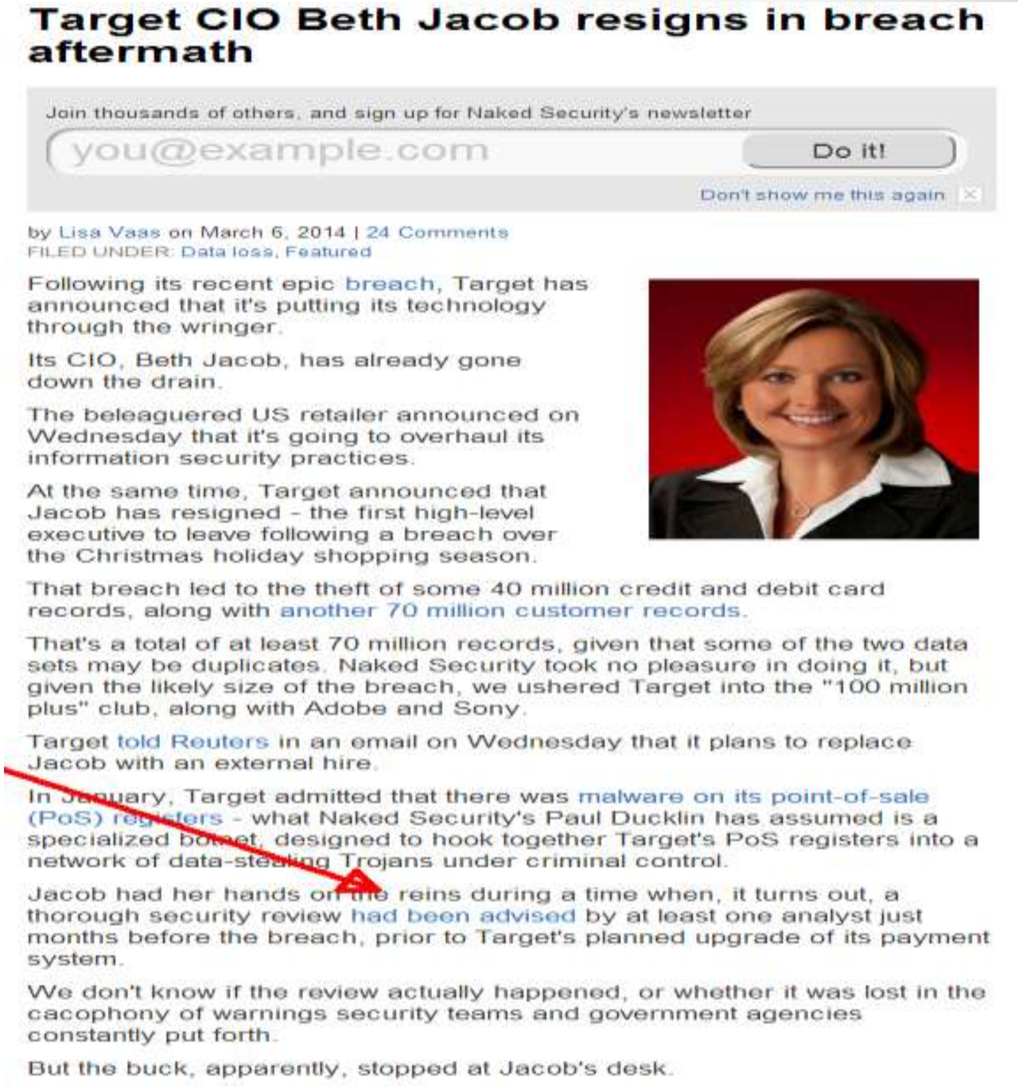
```
Of94-Eq_SP12-Item11-Pen8GB
  Part_1
    KINGSTON-FAT32
      a PALESTRAS
        Law_e_Medeiros.mpg
      CSP
        TURMA DELTA arquivos
          CURSO SUPERIOR DE POLICIA.zip
            CURSO SUPERIOR DE POLICIA
              CSP 2008 DPF
                Modelos Peti‡Æo Justi‡a
                  Textos interesse reconhecimento promo‡Æo
                    Arquivo Word
                      A‡Æo Cautelar (PEDIDOS).doc
      DriveFreeSpace05
        OLE_491520[19988]
      DriveFreeSpace13
        PNG_19832683[19996].png
      SATIAGRAHA
        ANA MARA CASO JORNALISTA
          JORNALISTA 2008-05-30 15-23-27 - 10 min 19 sec - 000000430000133100000000.wav
          Ofício nº 166 VAZAMENTO JORNAL.doc
          OPERAÇÃO SATIAGRAHA.doc
          Paulo e Queiroz em 09jul09_10h30mDW_B0017.wav
          Referência a AVNER SHEMESH.doc
        AUDIO E TRANSCRIÇOES
          Audio Dario
            Audio_04.04.2008 a 17.04.2008.doc
            Audio_15.05.2008 a.doc
            Audio_20.02.2008 a 26.02.2008.doc
          Transcricao Audio DVD
            Audio_CD_11.02.2008 a 29.02.2008.doc
          TRANSCRIÇÃO INTERCP TEL CD 11.02.2008 a 29.02.2008.doc
          Áudio do RJ em 27mai08
            2181697976_20080527131643_1_8339085.wav
        DADOS PARA VIGILÂNCIA
          ALVOS PRINCIPAIS e SECUNDARIOS.doc
          Atividade de GUIGA.doc
          Dúvidas sobre interlocutores de áudios solicitados em 19mai08.doc
          FICHAS DE ALVO RJ
            ARTHUR JOAQUIM DE CARVALHO.doc
            DANIEL VALENTE DANTAS_FICHA.doc
            DANIELE VIANA PREVITALI_FICHA.doc
            DANIELLE SILBERGLEID NINIO_FICHA.doc
```

Caso Target



Target is overhauling its information security practices, Gregg Steinhafel, the company's chairman, president and CEO, said in a statement. Target is searching for an interim CIO to help guide the company "through this transformation," he said.

In addition, Target is elevating its CISO role and hiring for that position and for a chief compliance offer, he added. The company has hired Promontory Financial Group "to help us evaluate our technology, structure, processes and talent as a part of this transformation," he said.



Target CIO Beth Jacob resigns in breach aftermath

Join thousands of others, and sign up for Naked Security's newsletter
you@example.com
Do it!
Don't show me this again

by Lisa Vaas on March 6, 2014 | 24 Comments
FILED UNDER: Data loss, Featured

Following its recent epic breach, Target has announced that it's putting its technology through the wringer.

Its CIO, Beth Jacob, has already gone down the drain.

The beleaguered US retailer announced on Wednesday that it's going to overhaul its information security practices.

At the same time, Target announced that Jacob has resigned - the first high-level executive to leave following a breach over the Christmas holiday shopping season.

That breach led to the theft of some 40 million credit and debit card records, along with another 70 million customer records.

That's a total of at least 70 million records, given that some of the two data sets may be duplicates. Naked Security took no pleasure in doing it, but given the likely size of the breach, we ushered Target into the "100 million plus" club, along with Adobe and Sony.

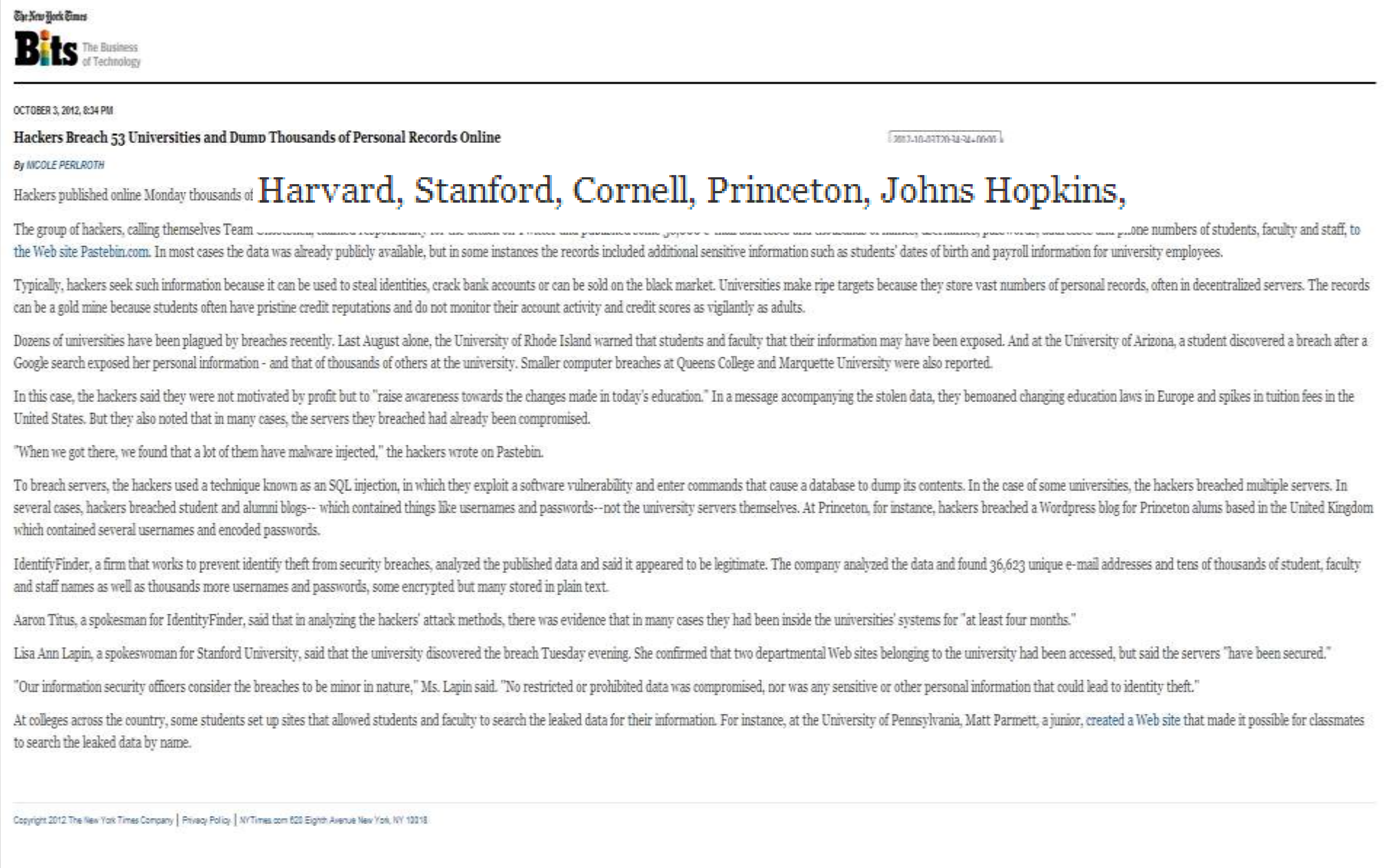
Target told Reuters in an email on Wednesday that it plans to replace Jacob with an external hire.

In January, Target admitted that there was malware on its point-of-sale (PoS) registers - what Naked Security's Paul Ducklin has assumed is a specialized botnet, designed to hook together Target's PoS registers into a network of data-stealing Trojans under criminal control.

Jacob had her hands on the reins during a time when, it turns out, a thorough security review had been advised by at least one analyst just months before the breach, prior to Target's planned upgrade of its payment system.

We don't know if the review actually happened, or whether it was lost in the cacophony of warnings security teams and government agencies constantly put forth.

But the buck, apparently, stopped at Jacob's desk.



The New York Times

Bits The Business of Technology

OCTOBER 3, 2012, 8:34 PM

Hackers Breach 53 Universities and Dump Thousands of Personal Records Online

2012-10-03T20:34:34+00:00

By NICOLE PERLROTH

Hackers published online Monday thousands of Harvard, Stanford, Cornell, Princeton, Johns Hopkins,

The group of hackers, calling themselves Team [illegible] ...one numbers of students, faculty and staff, to the Web site Pastebin.com. In most cases the data was already publicly available, but in some instances the records included additional sensitive information such as students' dates of birth and payroll information for university employees.

Typically, hackers seek such information because it can be used to steal identities, crack bank accounts or can be sold on the black market. Universities make ripe targets because they store vast numbers of personal records, often in decentralized servers. The records can be a gold mine because students often have pristine credit reputations and do not monitor their account activity and credit scores as vigilantly as adults.

Dozens of universities have been plagued by breaches recently. Last August alone, the University of Rhode Island warned that students and faculty that their information may have been exposed. And at the University of Arizona, a student discovered a breach after a Google search exposed her personal information - and that of thousands of others at the university. Smaller computer breaches at Queens College and Marquette University were also reported.

In this case, the hackers said they were not motivated by profit but to "raise awareness towards the changes made in today's education." In a message accompanying the stolen data, they bemoaned changing education laws in Europe and spikes in tuition fees in the United States. But they also noted that in many cases, the servers they breached had already been compromised.

"When we got there, we found that a lot of them have malware injected," the hackers wrote on Pastebin.

To breach servers, the hackers used a technique known as an SQL injection, in which they exploit a software vulnerability and enter commands that cause a database to dump its contents. In the case of some universities, the hackers breached multiple servers. In several cases, hackers breached student and alumni blogs-- which contained things like usernames and passwords--not the university servers themselves. At Princeton, for instance, hackers breached a Wordpress blog for Princeton alums based in the United Kingdom which contained several usernames and encoded passwords.

IdentifyFinder, a firm that works to prevent identify theft from security breaches, analyzed the published data and said it appeared to be legitimate. The company analyzed the data and found 36,623 unique e-mail addresses and tens of thousands of student, faculty and staff names as well as thousands more usernames and passwords, some encrypted but many stored in plain text.

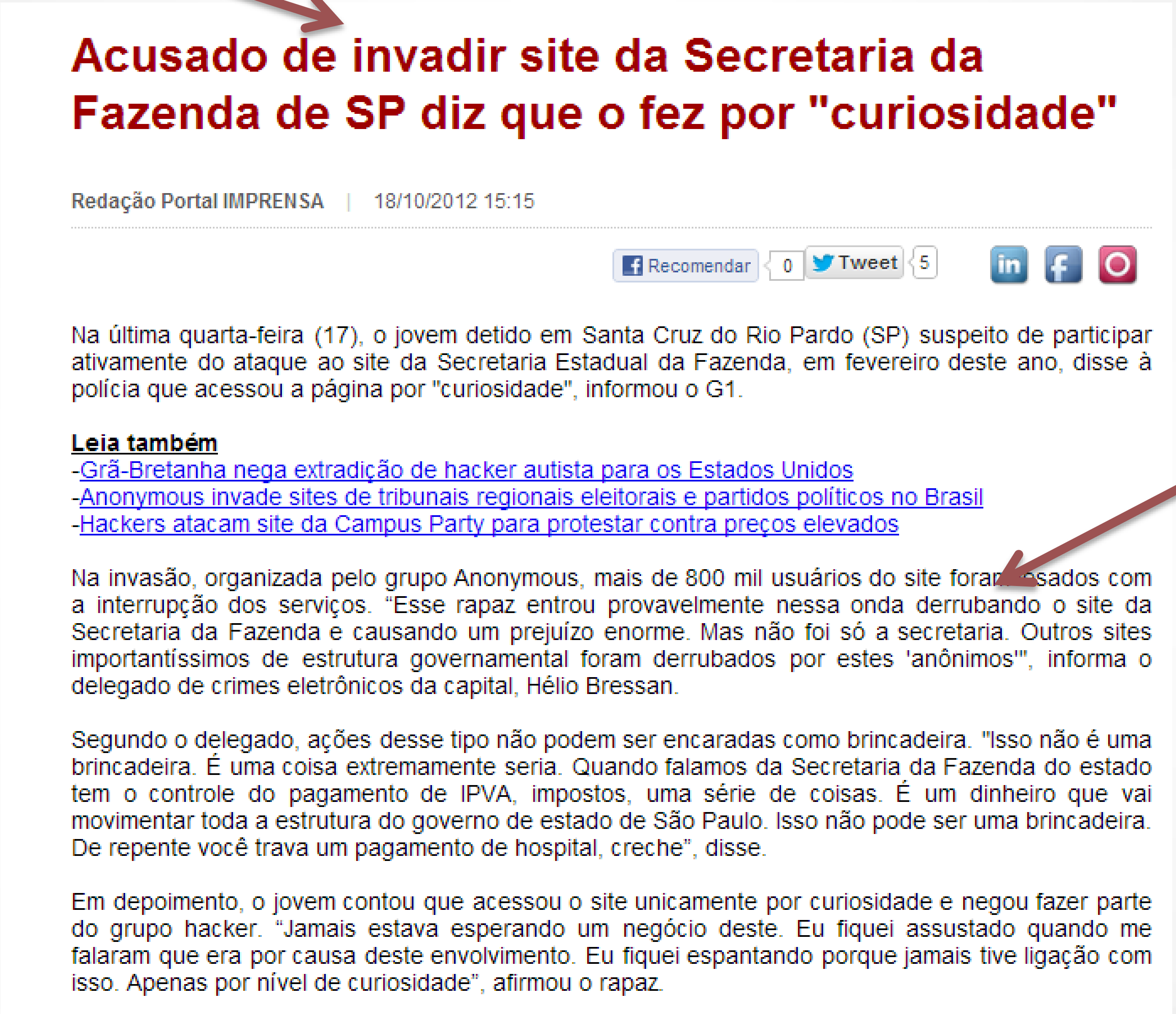
Aaron Titus, a spokesman for IdentityFinder, said that in analyzing the hackers' attack methods, there was evidence that in many cases they had been inside the universities' systems for "at least four months."

Lisa Ann Lapin, a spokeswoman for Stanford University, said that the university discovered the breach Tuesday evening. She confirmed that two departmental Web sites belonging to the university had been accessed, but said the servers "have been secured."

"Our information security officers consider the breaches to be minor in nature," Ms. Lapin said. "No restricted or prohibited data was compromised, nor was any sensitive or other personal information that could lead to identity theft."

At colleges across the country, some students set up sites that allowed students and faculty to search the leaked data for their information. For instance, at the University of Pennsylvania, Matt Parmett, a junior, created a Web site that made it possible for classmates to search the leaked data by name.

http://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records-online/



Acusado de invadir site da Secretaria da Fazenda de SP diz que o fez por "curiosidade"

Redação Portal IMPRENSA | 18/10/2012 15:15

Na última quarta-feira (17), o jovem detido em Santa Cruz do Rio Pardo (SP) suspeito de participar ativamente do ataque ao site da Secretaria Estadual da Fazenda, em fevereiro deste ano, disse à polícia que acessou a página por "curiosidade", informou o G1.

Leia também
-Grã-Bretanha nega extradição de hacker autista para os Estados Unidos
-Anonymous invade sites de tribunais regionais eleitorais e partidos políticos no Brasil
-Hackers atacam site da Campus Party para protestar contra preços elevados

Na invasão, organizada pelo grupo Anonymous, mais de 800 mil usuários do site foram lesados com a interrupção dos serviços. "Esse rapaz entrou provavelmente nessa onda derrubando o site da Secretaria da Fazenda e causando um prejuízo enorme. Mas não foi só a secretaria. Outros sites importantíssimos de estrutura governamental foram derrubados por estes 'anônimos'", informa o delegado de crimes eletrônicos da capital, Hélio Bressan.

Segundo o delegado, ações desse tipo não podem ser encaradas como brincadeira. "Isso não é uma brincadeira. É uma coisa extremamente seria. Quando falamos da Secretaria da Fazenda do estado tem o controle do pagamento de IPVA, impostos, uma série de coisas. É um dinheiro que vai movimentar toda a estrutura do governo de estado de São Paulo. Isso não pode ser uma brincadeira. De repente você trava um pagamento de hospital, creche", disse.

Em depoimento, o jovem contou que acessou o site unicamente por curiosidade e negou fazer parte do grupo hacker. "Jamais estava esperando um negócio deste. Eu fiquei assustado quando me falaram que era por causa deste envolvimento. Eu fiquei espantando porque jamais tive ligação com isso. Apenas por nível de curiosidade", afirmou o rapaz.

http://portalimprensa.uol.com.br/noticias/brasil/54337/acusado+de+invadir+site+da+secretaria+da+fazenda+de+sp+diz+que+o+fez+por+curiosidade

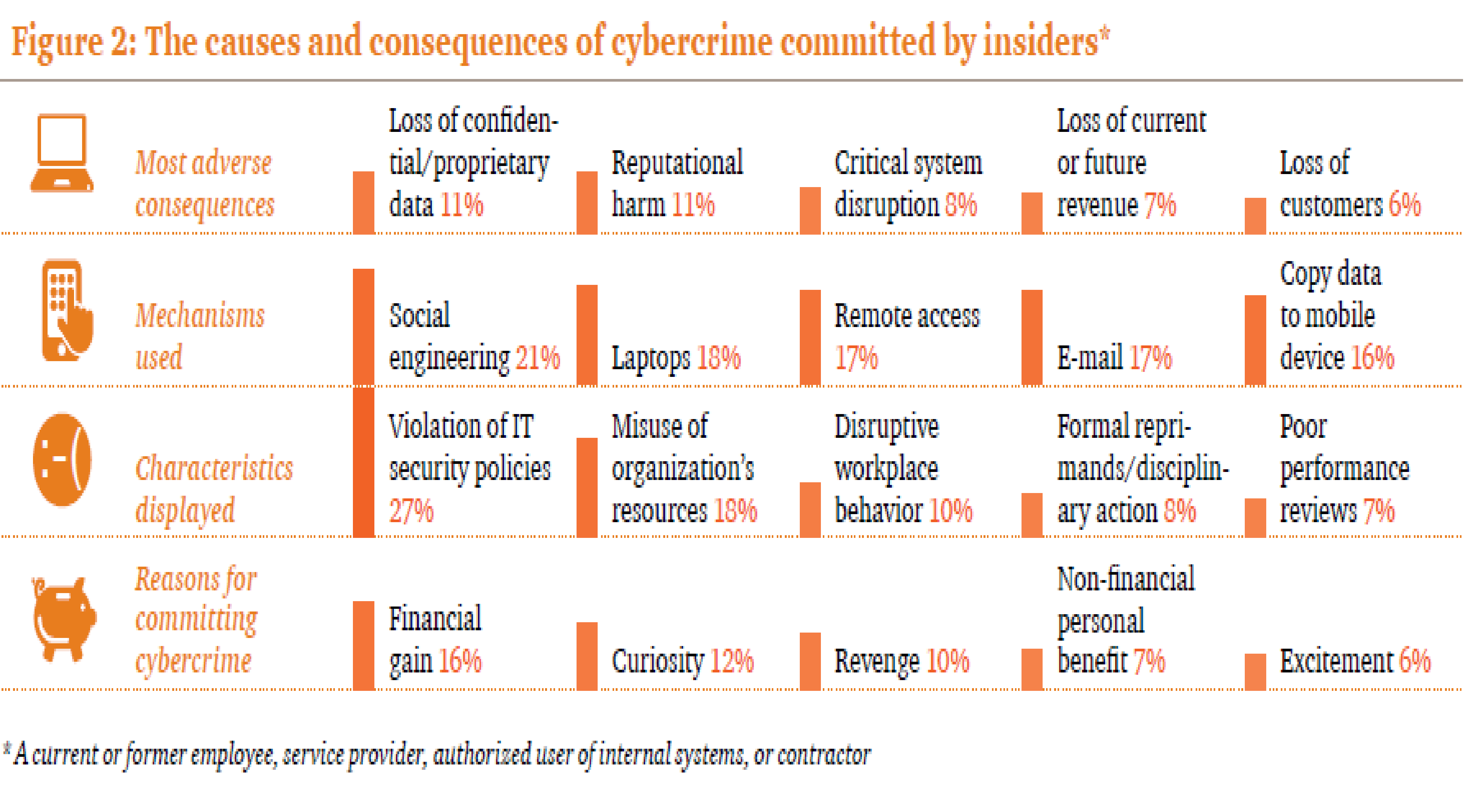
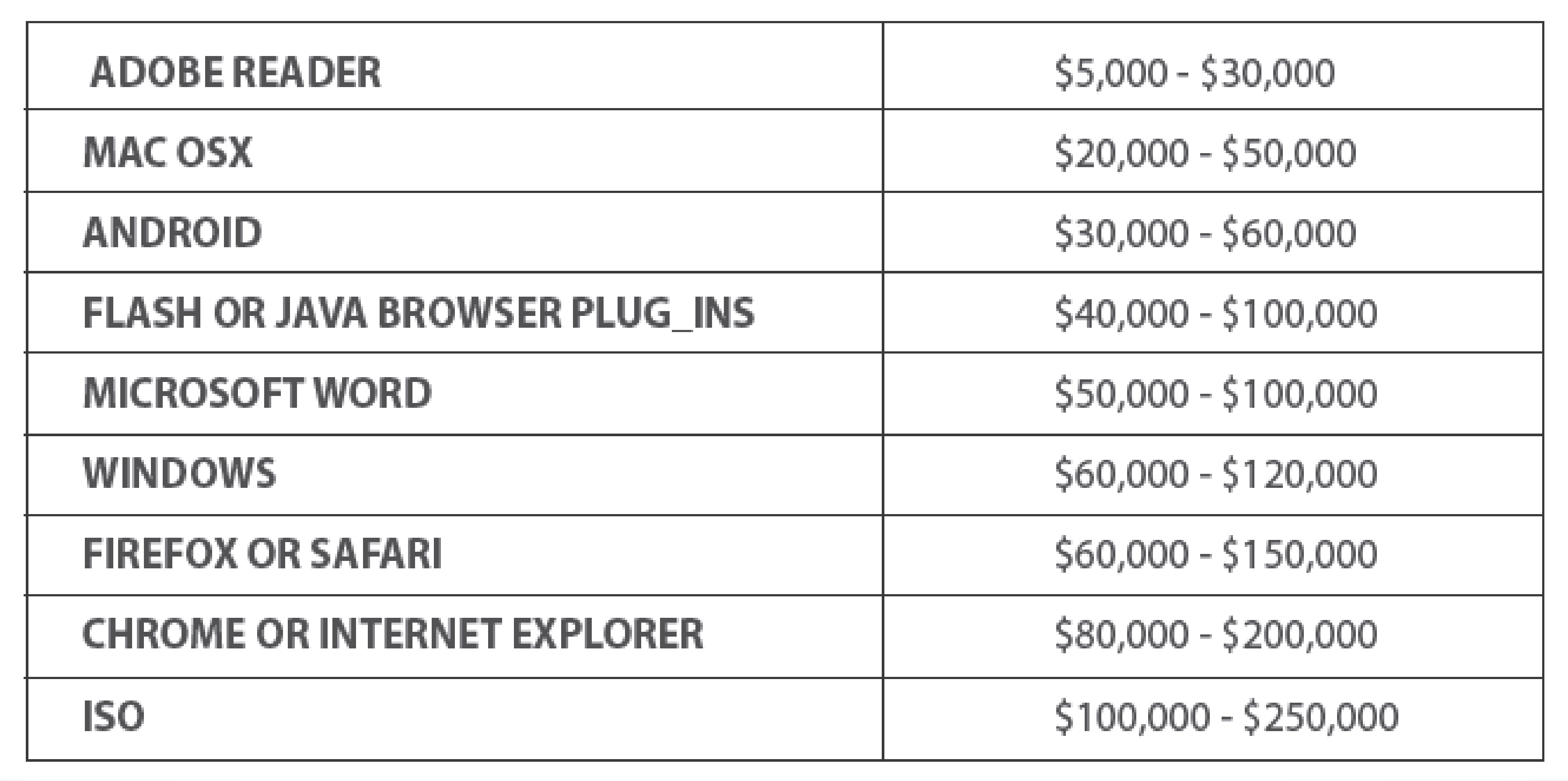


Figure 2: The causes and consequences of cybercrime committed by insiders*

Most adverse consequences	Loss of confidential/proprietary data 11%	Reputational harm 11%	Critical system disruption 8%	Loss of current or future revenue 7%	Loss of customers 6%
Mechanisms used	Social engineering 21%	Laptops 18%	Remote access 17%	E-mail 17%	Copy data to mobile device 16%
Characteristics displayed	Violation of IT security policies 27%	Misuse of organization's resources 18%	Disruptive workplace behavior 10%	Formal reprimands/disciplinary action 8%	Poor performance reviews 7%
Reasons for committing cybercrime	Financial gain 16%	Curiosity 12%	Revenge 10%	Non-financial personal benefit 7%	Excitement 6%

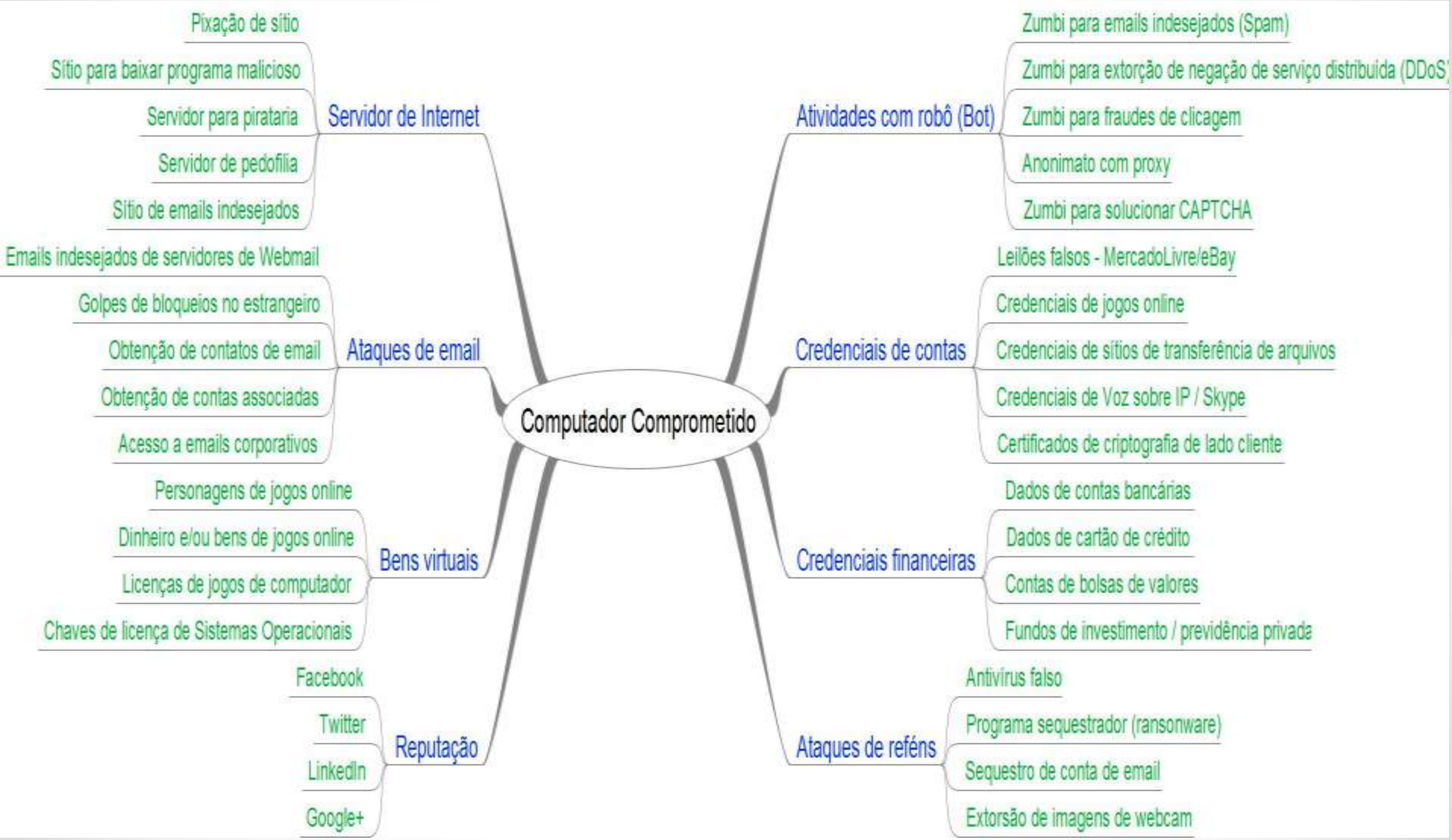
** A current or former employee, service provider, authorized user of internal systems, or contractor*

Fonte 2014 US State of Cybercrime Survey



ADOBE READER	$5,000 - $30,000
MAC OSX	$20,000 - $50,000
ANDROID	$30,000 - $60,000
FLASH OR JAVA BROWSER PLUG_INS	$40,000 - $100,000
MICROSOFT WORD	$50,000 - $100,000
WINDOWS	$60,000 - $120,000
FIREFOX OR SAFARI	$60,000 - $150,000
CHROME OR INTERNET EXPLORER	$80,000 - $200,000
ISO	$100,000 - $250,000

Black Market Value of Various Zero-Day Exploits (*Forbes)*



- Computador Comprometido
  - Servidor de Internet
    - Pixação de sítio
    - Sítio para baixar programa malicioso
    - Servidor para pirataria
    - Servidor de pedofilia
    - Sítio de emails indesejados
  - Ataques de email
    - Emails indesejados de servidores de Webmail
    - Golpes de bloqueios no estrangeiro
    - Obtenção de contatos de email
    - Obtenção de contas associadas
    - Acesso a emails corporativos
  - Bens virtuais
    - Personagens de jogos online
    - Dinheiro e/ou bens de jogos online
    - Licenças de jogos de computador
    - Chaves de licença de Sistemas Operacionais
  - Reputação
    - Facebook
    - Twitter
    - LinkedIn
    - Google+
  - Atividades com robô (Bot)
    - Zumbi para emails indesejados (Spam)
    - Zumbi para extorção de negação de serviço distribuida (DDoS)
    - Zumbi para fraudes de clicagem
    - Anonimato com proxy
    - Zumbi para solucionar CAPTCHA
  - Credenciais de contas
    - Leilões falsos - MercadoLivre/eBay
    - Credenciais de jogos online
    - Credenciais de sítios de transferência de arquivos
    - Credenciais de Voz sobre IP / Skype
    - Certificados de criptografia de lado cliente
  - Credenciais financeiras
    - Dados de contas bancárias
    - Dados de cartão de crédito
    - Contas de bolsas de valores
    - Fundos de investimento / previdência privada
  - Ataques de reféns
    - Antivírus falso
    - Programa sequestrador (ransonware)
    - Sequestro de conta de email
    - Extorsão de imagens de webcam

http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Formação Pericial

- Formação
  - Acadêmica e profissional (10.000 horas)
  - Legado de poucos profissionais
  - Sólida base em ciência da computação
  - Importância da experiência
  - Área de elevados níveis de confidencialidade
  - Conhecimentos multidisciplinares
    - TI, Jurídico, RH, Investigação, etc
  - Elevados investimentos
  - Certificações: devem ser um caminho e não um fim
  - Norma Complementar nº 17/IN01/DSIC/GSIPR

Questões Jurídicas

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

TÍTULO II
Dos Direitos e Garantias Fundamentais
CAPÍTULO I
DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

Art. 5º Todos são iguais perante a lei (…)

LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

Questões Jurídicas

- Legislação (Brasil)
  - Constituição
  - CPC
    - Artigos 145, 146 e 147
    - Artigo 420 e seguintes
  - Código de Defesa do Consumidor
  - Lei Geral das Telecomunicações
  - Decretos, Portarias, INs, etc

(…) http://dsic.planalto.gov.br/legislacaodsic

Oportunidades e desafios

- Por que uma empresa precisa de perícia forense corporativa?
  - Crime organizado transnacional
  - Funcionários insatisfeitos
  - Falta conscientização de usuários
  - Forças policiais com diversas limitações
  - Anarquistas digitais
  - Ferramentas *hackers* amplamente disponíveis
  - *Operação Aurora, Stuxnet*...

Oportunidades e desafios

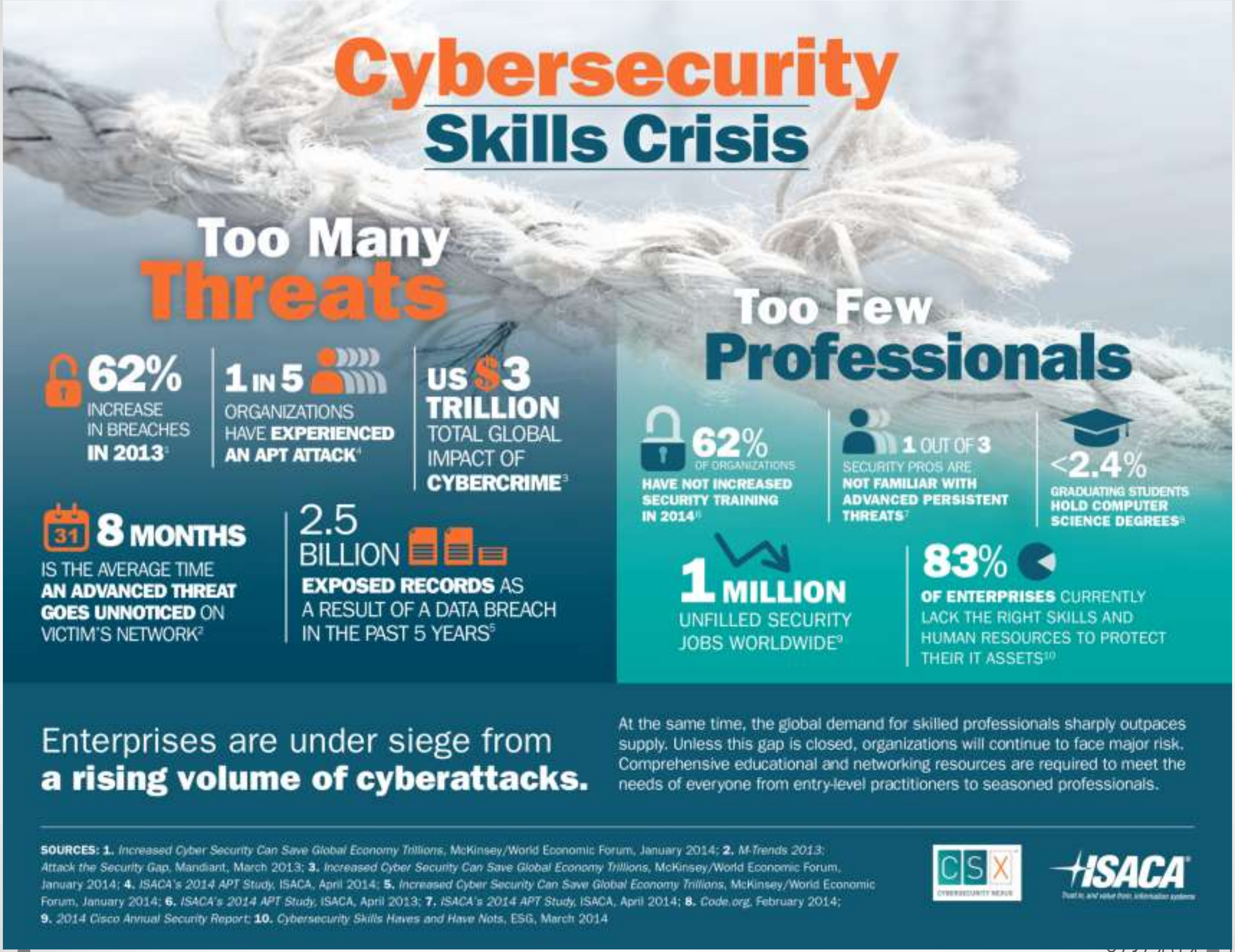
- Efeito CSI
- Restrições orçamentárias: hardware, software, treinamento, certificações, pessoal
- Falta de pessoal especilizado, de uma equipe formal de resposta a incidentes e de estratégias
- Novas mídias
- Backlogs

Oportunidades e desafios

- Manuseio das evidências => Cadeia de Custódia
- Utilização de criptografia e anti-forense
- MOM
- Questões legais
- APTs, *Cloud computing*, *ransonware*, *sink hole*, consumerização, *big data*, extorsão DDoS, *Deep Web*, *script kiddies*, *porn revenge*, hacktivismo, *cybersquatting*, etc.

Oportunidades e desafios

- Profissionais brasileiros de TI dão um "jeitinho" em quase tudo
- A teoria do pato
  - – Não voa direito
  - – Não anda direto
  - – Não nada direito
  - – …



Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF **3** SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% GRADUATING STUDENTS **HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

http://www.businesswire.com/news/home/20140428005631/en/Address-Global-Cybersecurity-Skills-Crisis-ISACA-Unveils

Links úteis

- DFIR (Digital Forensics and Incident Response) http://dfir.com.br
- HTCIA Brasilia - http://www.facebook.com/HTCIABrasilia
- Schneier on Security - https://www.schneier.com/
- Krebs on Security - http://krebsonsecurity.com/
- SANS Institute Blogs - http://www.sans.org/security-resources/blogs

Para concluir...

"Existem apenas dois tipos de empresas: as que foram hackeadas, e aquelas que serão. Mesmo isto está se fundindo em uma categoria: as que foram hackeadas e serão novamente."

ROBERT MUELLER – Diretor do FBI

Perguntas

marcelobc@mpf.mp.br