KPMG

Cyber Incident Preparedness and the Current Cyber Threat Landscape

Iain D. Kenny, CISSP, CCE, CFE, CAMS

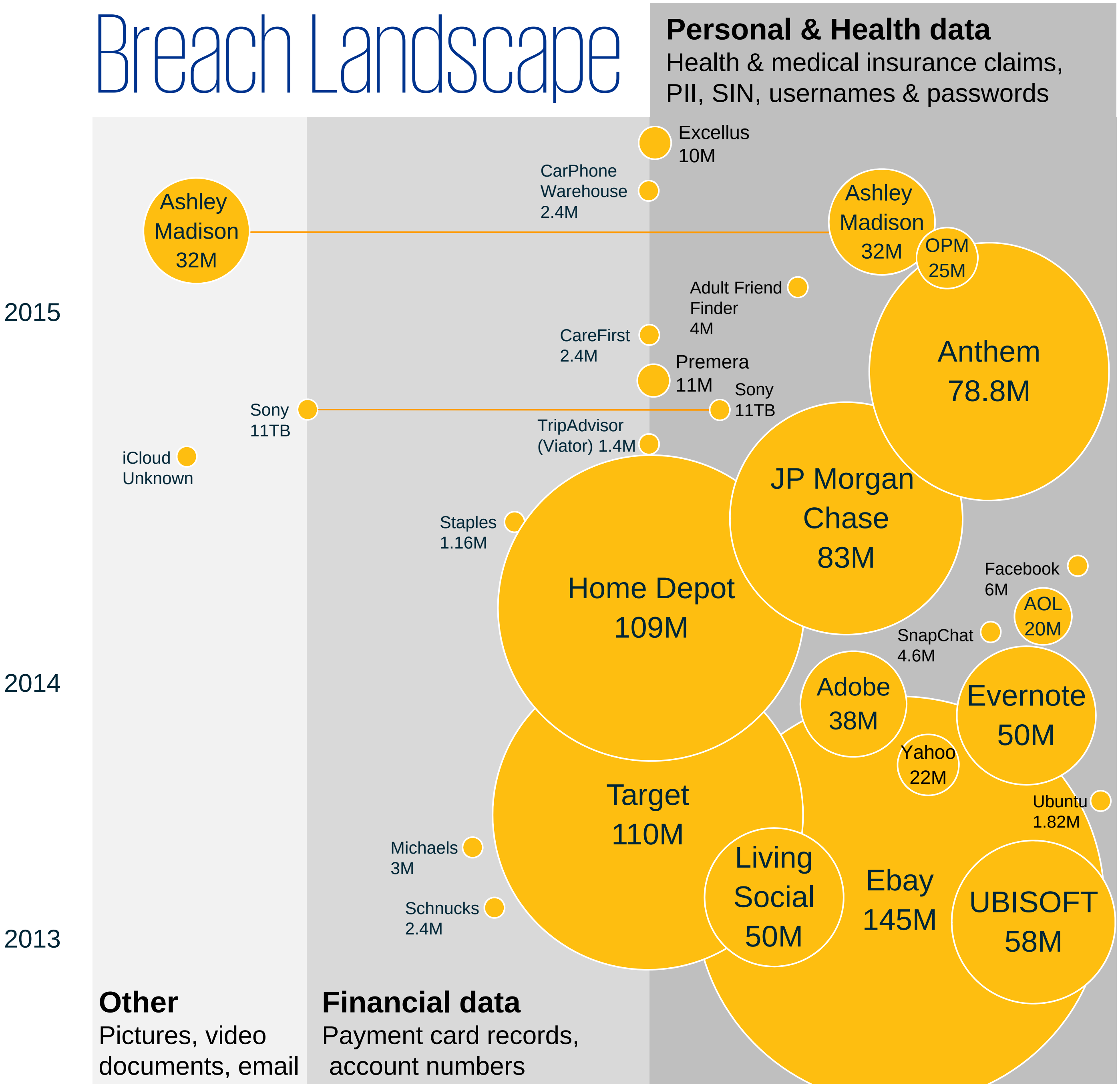
Partner, Risk Consulting & National Digital Forensics Leader

Tel: (403) 978-4765
Email: ikenny@kpmg.ca

- Former Technological Crimes Detective (Edmonton Police Service)
- Court declared expert in Digital Evidence Preservation and Analysis

The Breach Landscape

Breach Landscape



Top data breaches 2013 – Sept. 15, 2015

Data breaches of recognized companies involving at least 1M records by size and type

High-demand data within the underground economy

- Personal & health data
- Usernames & passwords
- Loyalty reward points
- Social media accounts
- Financial data

Breach Landscape

Impact of a typical breach

Average cost (CAD) of a breach 5.32M or $250 per record

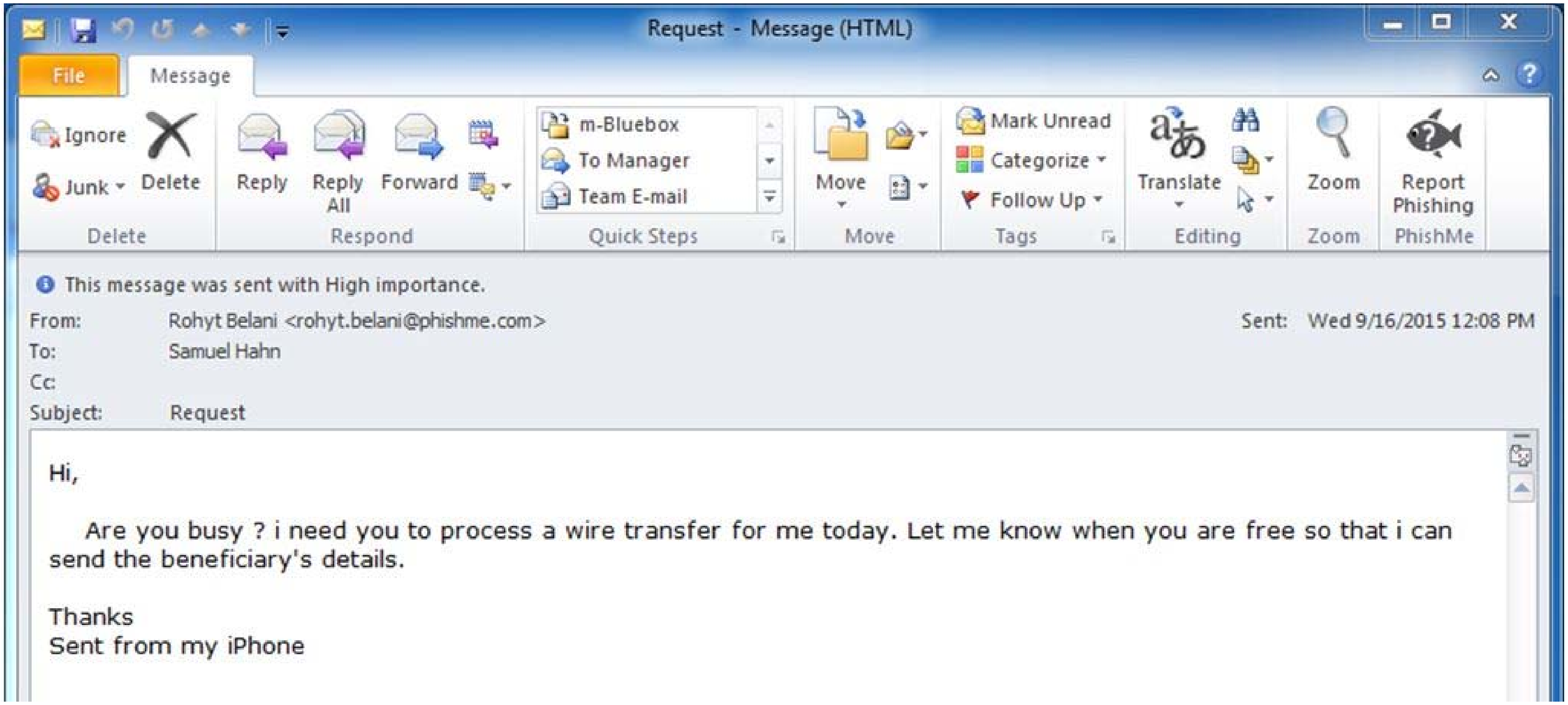
1.68M	Detection & Escalation
.12M	Notification
1.53M	Post-breach services
1.99M	Lost business

Source: The Ponemon Institute's "2015 Cost of Data Breach Study: Canada"

Current Threats

Executive Impersonation Fraud

Executive fraud – where a criminal poses as a senior person within the firm, either by hacking or "spoofing" their email account, and convinces someone with financial authority to make a payment.



This message was sent with High importance.

From: Rohyt Belani <rohyt.belani@phishme.com>

Sent: Wed 9/16/2015 12:08 PM

To: Samuel Hahn

Cc:

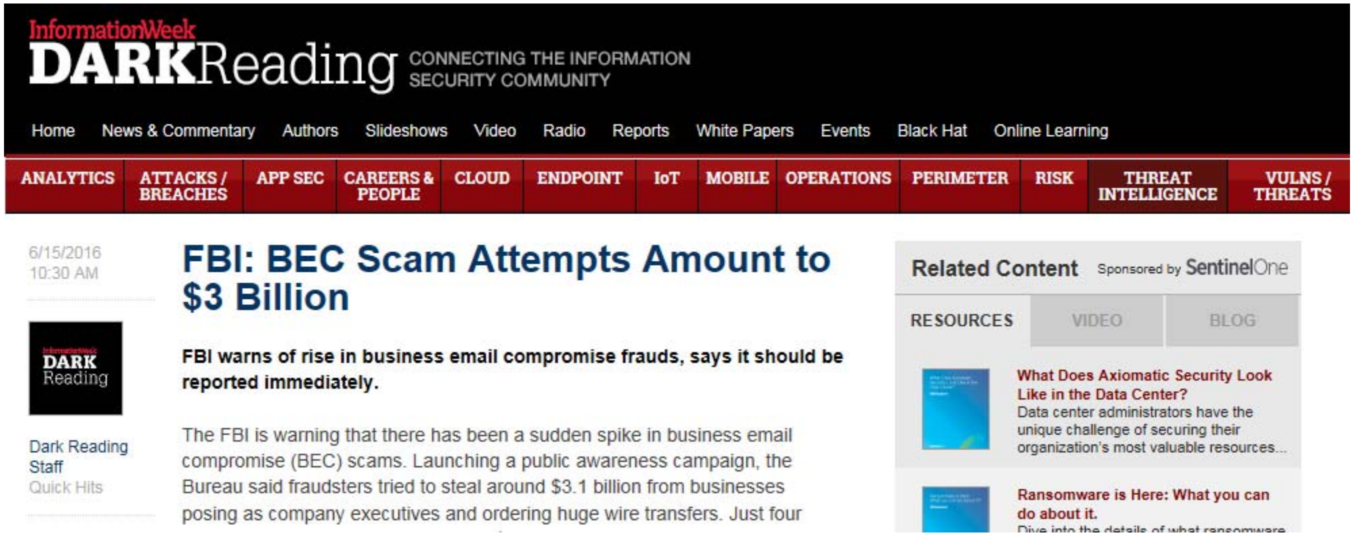
Subject: Request

Hi,

Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my iPhone

Executive Impersonation Fraud



6/15/2016
10:30 AM

Dark Reading Staff
Quick Hits

FBI: BEC Scam Attempts Amount to $3 Billion

FBI warns of rise in business email compromise frauds, says it should be reported immediately.

The FBI is warning that there has been a sudden spike in business email compromise (BEC) scams. Launching a public awareness campaign, the Bureau said fraudsters tried to steal around $3.1 billion from businesses posing as company executives and ordering huge wire transfers. Just four

What Does Axiomatic Security Look Like in the Data Center?
Data center administrators have the unique challenge of securing their organization's most valuable resources...

Ransomware is Here: What you can do about it.
Dive into the details of what ransomware

Recovering from executive impersonation fraud

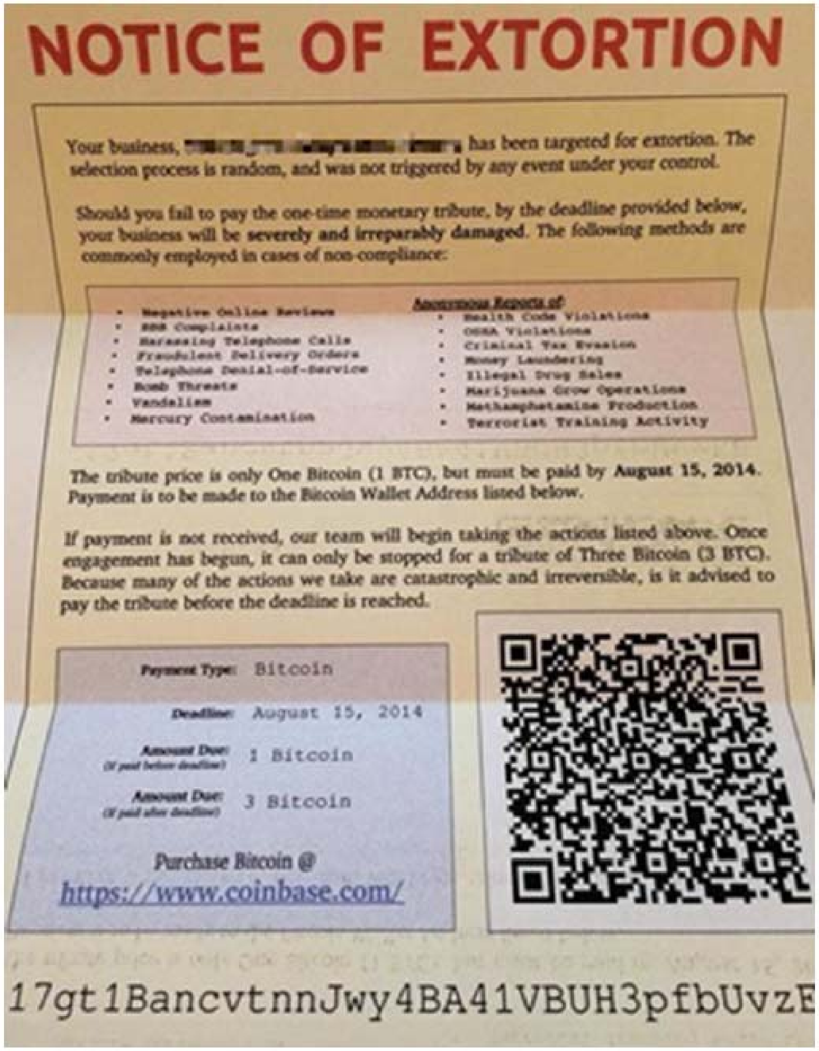
1) Do not reply to the email
2) Take steps to independently confirm the legitimacy of the instructions
3) Inform organizational management
4) Immediately make employees aware
5) Engage a forensics provider to attempt to identify origin and insider involvement
6) Check historical financial / data transfers for past attacks
7) Examine workflow systems for malware
8) Review the adequacy of internal controls to combat future attempts

Extortion Driven Attacks of Today

Cyber Extortion – Where an individual receives threats in relation to the leak of sensitive and often embarrassing information. Perpetrators demand nominal payment to avoid exposure.

Ransomware – where a piece of malicious software, typically received via a phishing email, encrypts all of the data on the company's network, with the perpetrators requesting a ransom in order to provide the decryption key.

- Usually payments are requested in Bitcoins



NOTICE OF EXTORTION

Your business, [redacted] has been targeted for extortion. The selection process is random, and was not triggered by any event under your control.

Should you fail to pay the one-time monetary tribute, by the deadline provided below, your business will be **severely and irreparably damaged**. The following methods are commonly employed in cases of non-compliance:

- Negative Online Reviews
- BBB Complaints
- Harassing Telephone Calls
- Fraudulent Delivery Orders
- Telephone Denial-of-Service
- Bomb Threats
- Vandalism
- Mercury Contamination

Anonymous Reports of:

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion
- Money Laundering
- Illegal Drug Sales
- Marijuana Grow Operations
- Methamphetamine Production
- Terrorist Training Activity

The tribute price is only One Bitcoin (1 BTC), but must be paid by **August 15, 2014**. Payment is to be made to the Bitcoin Wallet Address listed below.

If payment is not received, our team will begin taking the actions listed above. Once engagement has begun, it can only be stopped for a tribute of Three Bitcoin (3 BTC). Because many of the actions we take are catastrophic and irreversible, is it advised to pay the tribute before the deadline is reached.

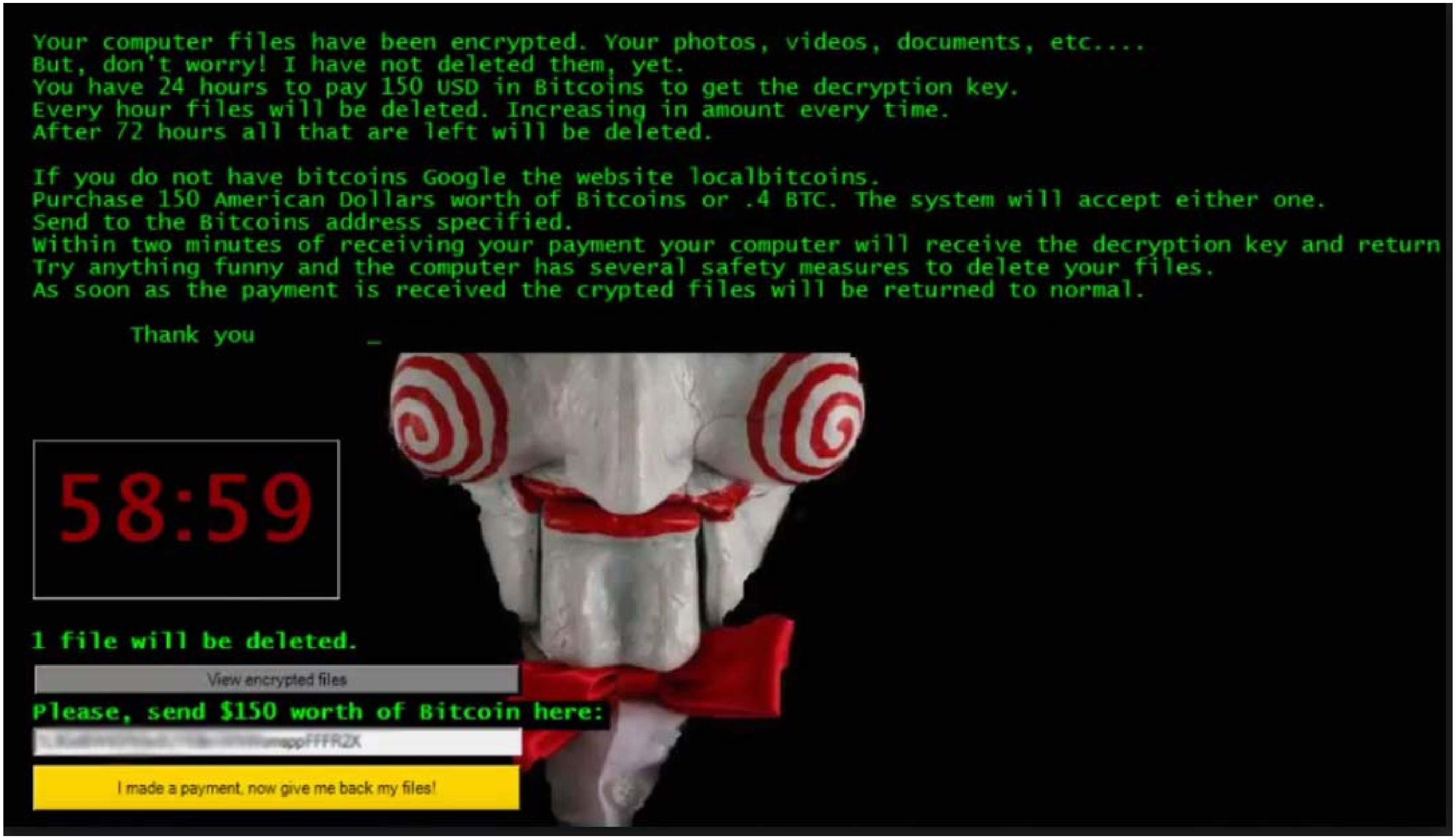
Payment Type:	Bitcoin
Deadline:	August 15, 2014
Amount Due: (If paid before deadline)	1 Bitcoin
Amount Due: (If paid after deadline)	3 Bitcoin

Purchase Bitcoin @
https://www.coinbase.com/

17gt1BancvtnnJwy4BA41VBUH3pfbUvzE

Source: Data Breach Preparation & Response, Kevvie Fowler (ISBN: 0128034513)

Extortion Driven Attacks of Today



```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.

        Thank you
```

58:59

1 file will be deleted.

Please, send $150 worth of Bitcoin here:

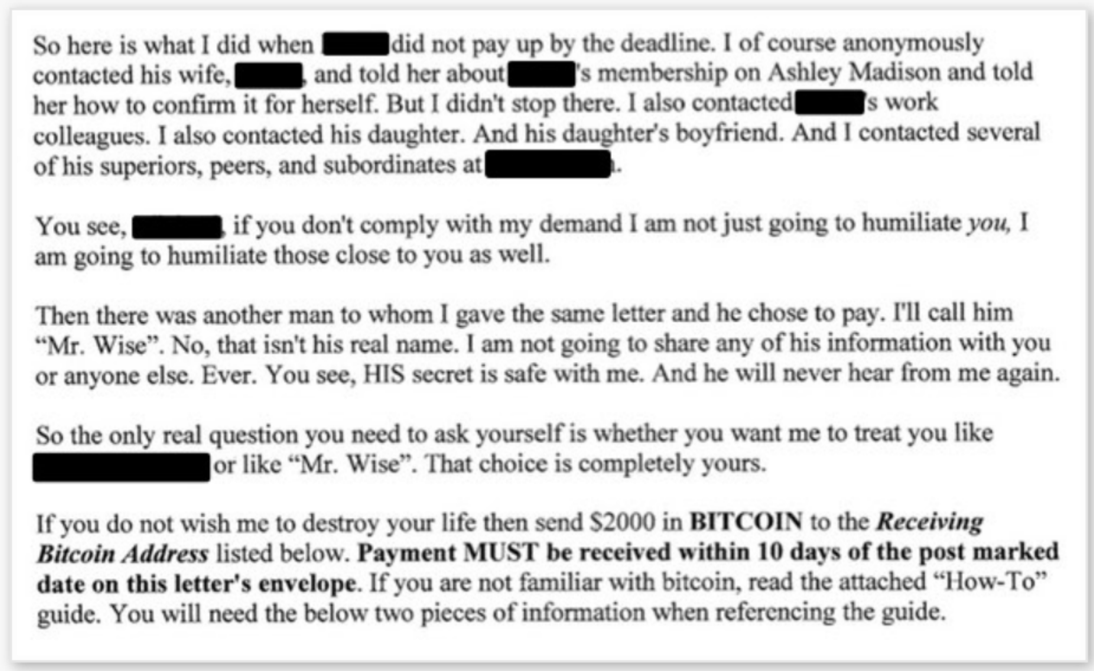
[redacted]mppFFFR2X

Source: http://sensorstechforum.com/remove-jigsaw-ransomware-and-restore-fun-kkk-btc-encrypted-files/

Extortion Driven Attacks of Today

Spouses of Ashley Madison users targeted with blackmail letters

Threatening letters sent to the partners of former and current members, as well as themselves, with the demand: ‘pay $2,500 in bitcoin or have your infidelity exposed’



So here is what I did when [redacted] did not pay up by the deadline. I of course anonymously contacted his wife, [redacted], and told her about [redacted]'s membership on Ashley Madison and told her how to confirm it for herself. But I didn't stop there. I also contacted [redacted]'s work colleagues. I also contacted his daughter. And his daughter's boyfriend. And I contacted several of his superiors, peers, and subordinates at [redacted].

You see, [redacted], if you don't comply with my demand I am not just going to humiliate *you,* I am going to humiliate those close to you as well.

Then there was another man to whom I gave the same letter and he chose to pay. I'll call him “Mr. Wise”. No, that isn't his real name. I am not going to share any of his information with you or anyone else. Ever. You see, HIS secret is safe with me. And he will never hear from me again.

So the only real question you need to ask yourself is whether you want me to treat you like [redacted] or like “Mr. Wise”. That choice is completely yours.

If you do not wish me to destroy your life then send $2000 in **BITCOIN** to the ***Receiving Bitcoin Address*** listed below. **Payment MUST be received within 10 days of the post marked date on this letter's envelope**. If you are not familiar with bitcoin, read the attached “How-To” guide. You will need the below two pieces of information when referencing the guide.

Source: https://www.theguardian.com/technology/2016/mar/03/ashley-madison-users-spouses-targeted-by-blackmailers

KPMG

Extortion Driven Attacks of Today

Recovering from Ransomware

1) Do not turn off infected systems
2) Engage a cyber forensics team immediately
3) Limit the access of infected systems
4) Restrict interzone and system-to-system direct access
5) Protect backups
6) Warn other employees
7) Identify the type of ransomware
8) Identify the source of infection
9) It's a business decision on ransom payment
10) Bolster cyber security to limit the likelihood of a repeat occurrence

Recovering from cyber extortion

Organizations

1) Identify point of unauthorized access
2) Sever unauthorized access
3) Check email and firewall logs for other criminal communication with other employees likely being blackmailed
4) Proactively search breach databases for employees at risk of cyber extortion

Individuals

1) Face it, criminals will likely not go away
2) Sever unauthorized access
3) Contact law enforcement
4) By cyber aware
5) Bolster cyber security to limit the likelihood of a repeat occurrence

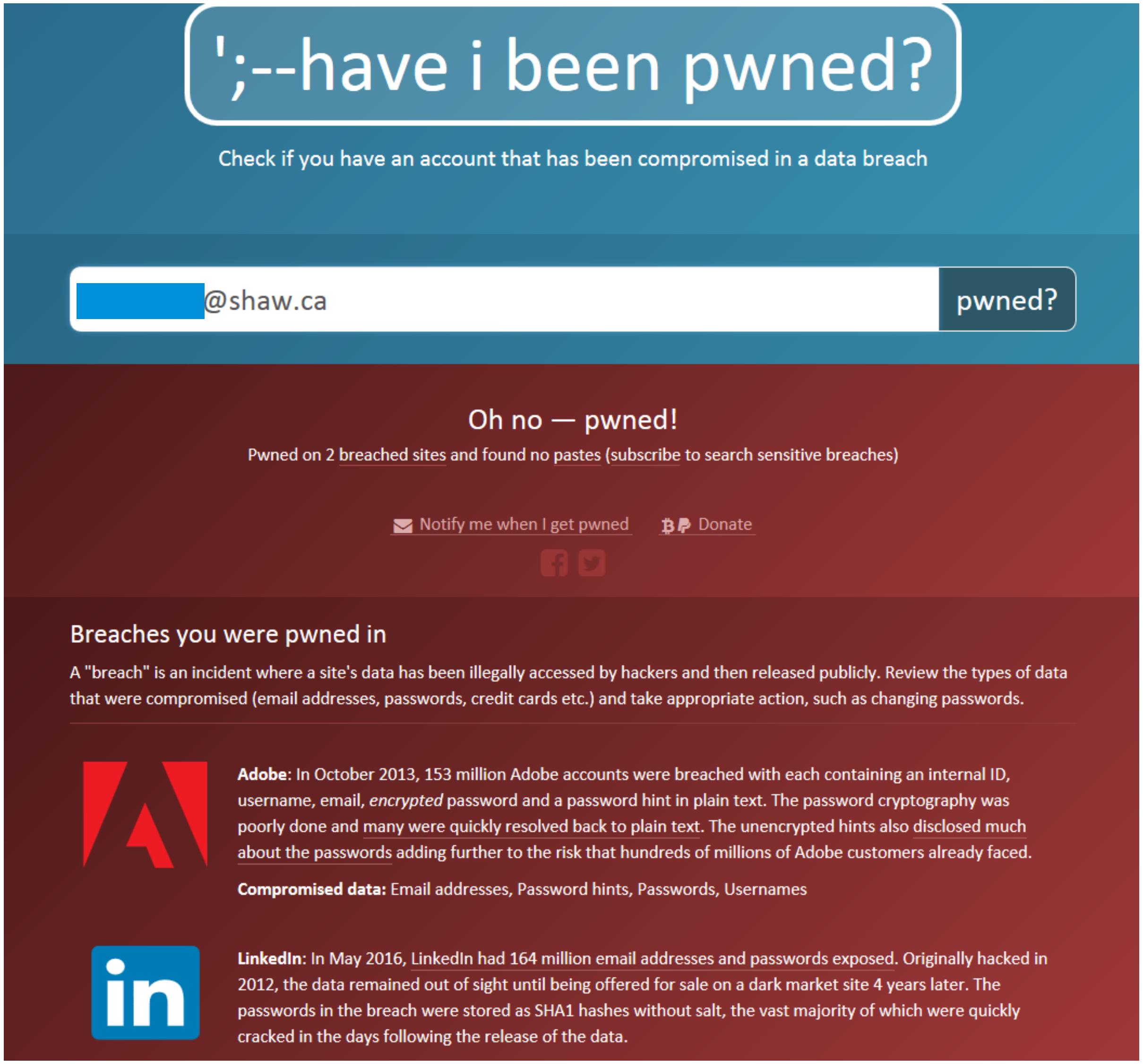
Have I been Pwned?

haveibeenpwned.com

pwned
A corruption of the word "Owned." This originated in an online game called Warcraft, where a map designer misspelled "owned." When the computer beat a player, it was supposed to say, so-and-so "has been owned."

Instead, it said, so-and-so "has been pwned."

haveibeenpwned.com tracks major data breaches and publicly released information to check if your credentials have been exposed



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

[redacted]@shaw.ca

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

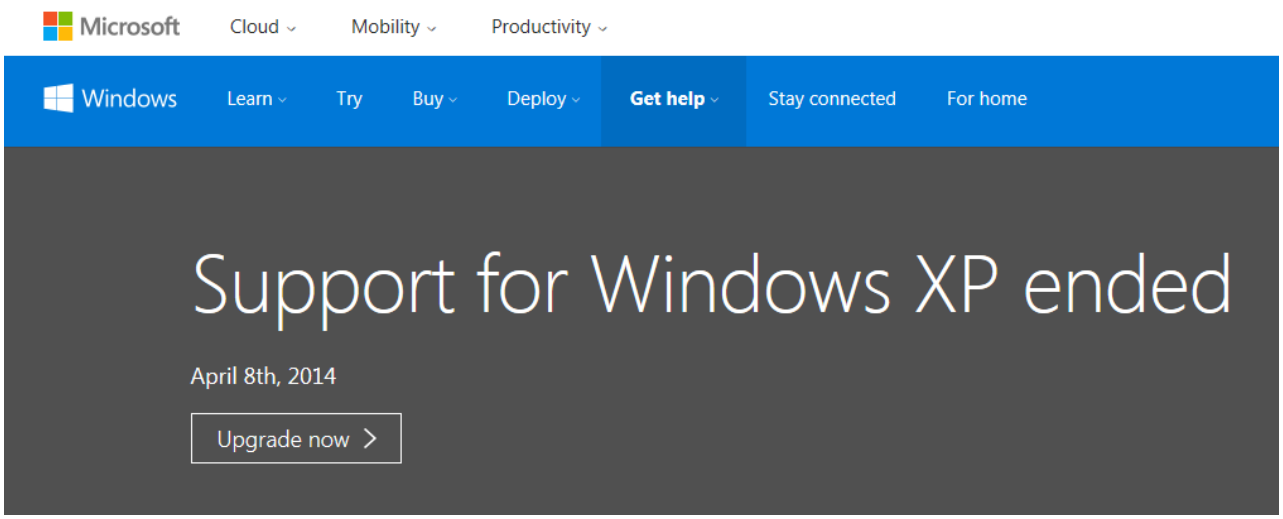
Compromised data: Email addresses, Password hints, Passwords, Usernames

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

http://www.urbandictionary.com/define.php?term=pwned&defid=94413

Hacking

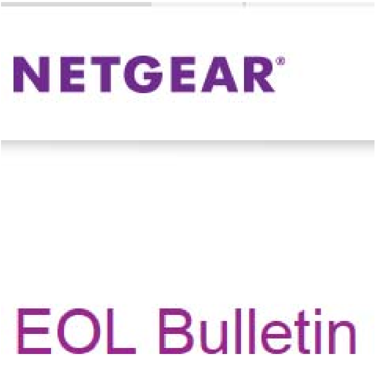
Hack attack – where a hacker gains access to the company's network, typically by exploiting an unpatched vulnerability within the software, allowing them access to the company data. The target will generally be personally identifiable information (PII) on a company's customers, especially credit card information



Support for Windows XP ended

April 8th, 2014

Source https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support

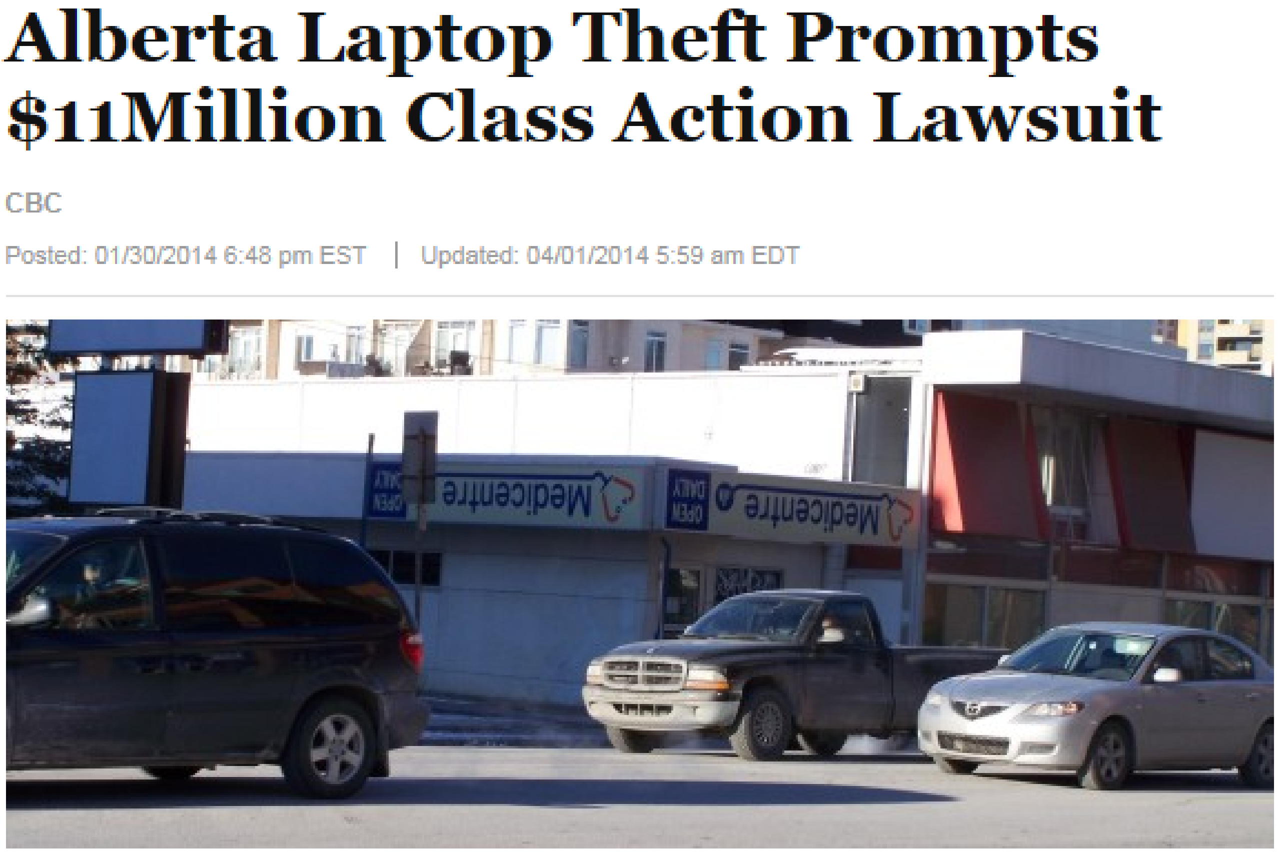


EOL Bulletin

Source
http://www.netgear.com/landing/eol.aspx?cid=wmt_netgear_organic

Loss of intellectual Property

- **Loss of unencrypted data through theft or loss of device**



Alberta Laptop Theft Prompts $11Million Class Action Lawsuit

CBC

Posted: 01/30/2014 6:48 pm EST | Updated: 04/01/2014 5:59 am EDT

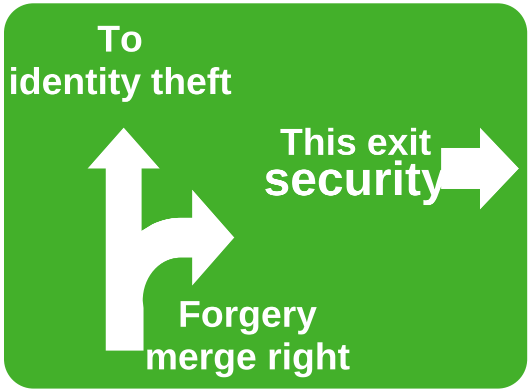
http://www.huffingtonpost.ca/2014/01/30/health-information-theft-medicentres-lawsuit_n_4698931.html

Preparing for the Inevitable

How to get Cyber security right

Build a Cyber Defensible Position

Build a Cyber defensible position to demonstrate proper organizational due diligence in:



- Preventing a security incident:
  - Identifying sensitive information and organizational requirements to protect it
  - Ensuring the proper governance and operational management of data
  - Protecting security findings from future data breach litigation
- Detecting and recovering from a security incident:
  - Self-identifying a security incident
  - Effectively responding, recovering and notifying affected individuals
- Helping to ensure a repeat related security incident isn't experienced:
  - Improve resiliency after an incident

The result:

- A reduction in the likelihood or magnitude of fines from regulators, clients, partners and government bodies
- A reduction in the backlash from customers who may otherwise take their business elsewhere
- A reduction in the impact to share-price and the reaction to this from shareholders
- Less attention paid to your breach by the media
- Overall protection of your brand

Breach Preparation

1 Define sensitive data

Define what is important to your organization and the hackers.

2 Identify breach scenarios

Perform a Threat Risk Assessment (TRA)

- Identify threats, vulnerabilities and likelihood of exploitation
- Develop breach scenarios

3 Assess detection & response capabilities

Assess your organization's ability to manage an incident

- Threat/incident detection
- Efficiency and accuracy of response
- Computer Security Incident Response Team structure and effectiveness
- Performance metrics

4 Develop / refresh your response plan

Identify a target state and address gaps to allow your organization to better detect and manage incidents

- Time to discover
- Time to manage
- Severity of post mortem review findings

5 Test and improve the response program

Develop a testing strategy that includes key internal and external CSIRT responders

- Live-fire testing
- Table-top testing
- Event simulations

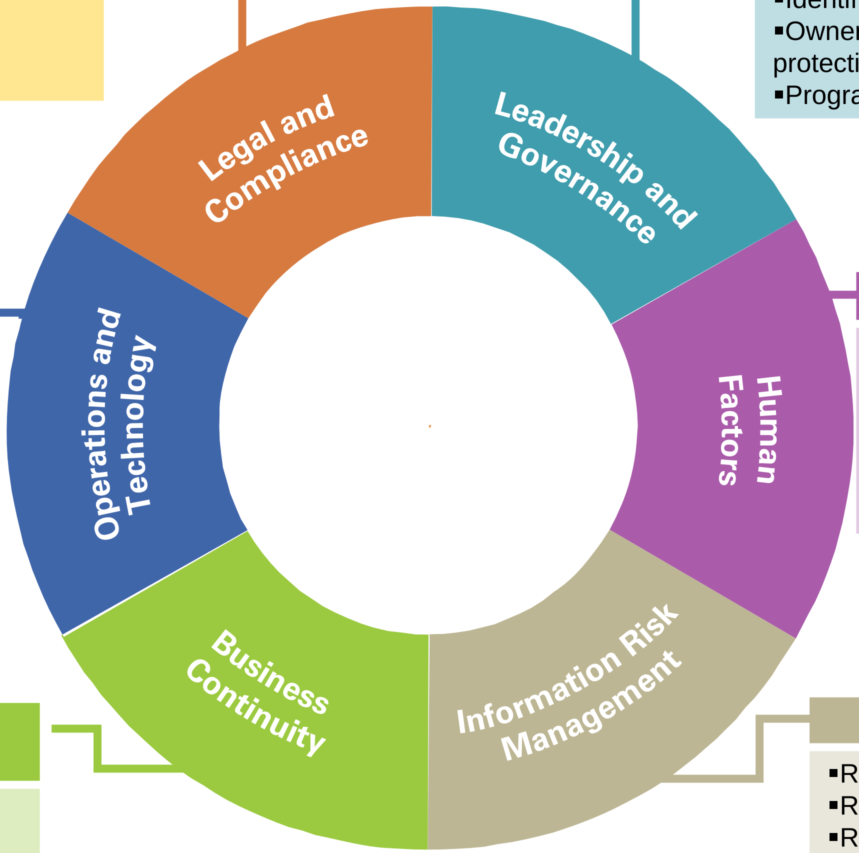
A Whole Business Approach to Cyber Security

Legal and Compliance

- Inventory of compliance requirements
- Compliance program components
- Role of the Audit Committee
- Litigation inventory
- Cyber insurance

Leadership and Governance

- Board involvement
- Third-party supplier relationships
- Identification of critical data
- Ownership and governance for data protection
- Program management


Legal and Compliance
Leadership and Governance
Human Factors
Information Risk Management
Business Continuity
Operations and Technology

Operations and Technology

- Threat and vulnerability management
- Logical security controls
- Physical security controls
- Security monitoring
- Incident response
- Integration with IT service management

Human Factors

- Training and awareness
- Culture
- Personnel security measures
- Talent management
- Organizational roles and responsibilities

Business Continuity and Crisis Management

- Ability to manage cyber events
- Financial ramifications and budget
- Resources required and training
- Detailed plans
- Communications
- Testing

Information Risk Management

- Risk management approach and policies
- Risk tolerance identification
- Risk assessment and measures
- Change management
- Information sharing
- Third party accreditation
- Information communication architecture

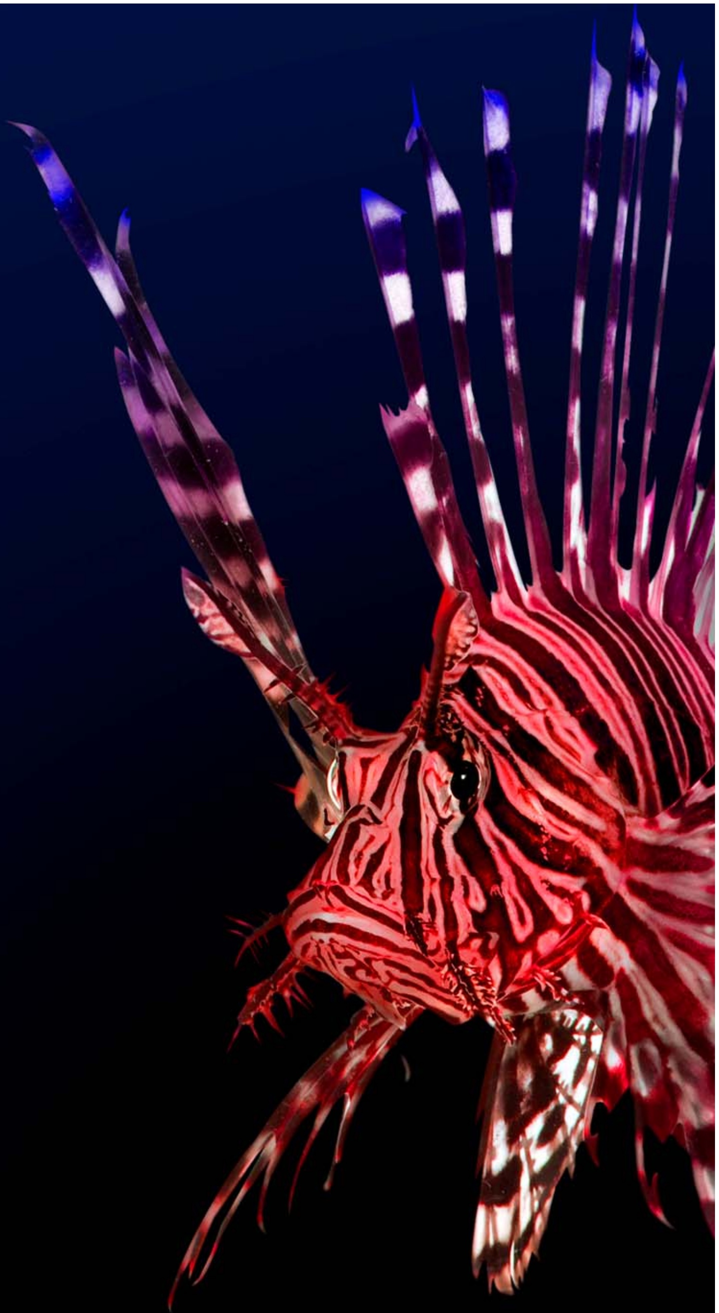
Thank You

Iain D. Kenny, **CISSP, CCE, CFE, CAMS**

Partner, Risk Consulting &

National Digital Forensics Leader

Tel: (403) 691-8489
Cell: (403) 978-4765
Email: ikenny@kpmg.ca



KPMG

kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.