



Grant Thornton

An instinct for growth™

# Cybersecurity

*Asset managers in the crosshairs*

30 September 2015

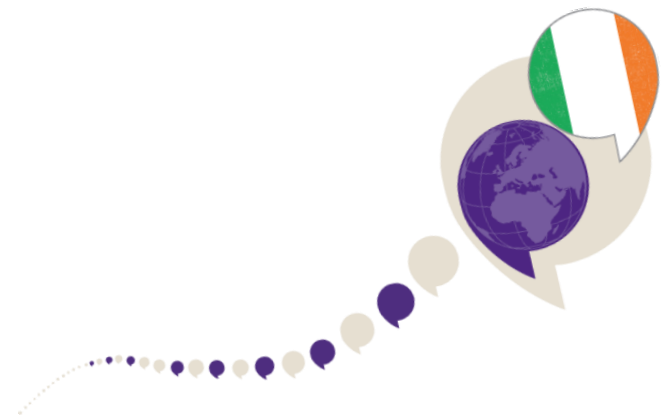
**Andy Harbison**

Director – IT Forensics Lead  
Grant Thornton Ireland



# Agenda

- introduction
- what is the problem?
- how should you respond?



# Introduction



# Focus

ft.com > companies > financials >

## Financial Services

Home World Companies Markets Global Economy Lex  
Energy Financials Health Industrials Luxury 360 Media Retail & Consumer Tech

May 10, 2015 11:48 am

### US government warns hedge funds pose cyber risk

Stephen Foley in Las Vegas

Share Author alerts Print Clip Comments



IM

## Guidance Update

APRIL 2015 | No. 2015-02

### CYBERSECURITY GUIDANCE

The Division has identified the cybersecurity of registered investment companies ("funds") and registered investment advisers ("advisers") as an important issue. Both funds and advisers increasingly use technology to conduct their business activities and need to protect confidential and sensitive information related to these activities from third parties, including information concerning fund investors and advisory clients. This guidance update highlights the importance of the issue and discusses a number of measures that funds and advisers may wish to consider when addressing cybersecurity risks. Because of the rapidly changing nature of cyber threats, the Division will continue to focus on cybersecurity and monitor events in this area.



# Regulator

FINANCIAL TIMES Monday 25 May 2015

FTfm | 5

## NEWS

# Ireland reviews cyber security of fund houses

### CYBER CRIME

Central bank has begun carrying out on-site inspections

ATTRACTA MOONEY AND MADISON MARRIAGE

Ireland's financial watchdog has launched a review of the cyber security policies and procedures of asset managers, amid fears that the investment industry has been painfully slow to tackle the threat of cyber crime.

of businesses. They were chosen randomly from those who had responded to a questionnaire about cyber security sent out by the regulator last month.

Last year the Bank of England warned that UK financial services companies were underestimating the danger of cyber attacks. It said financial companies tended to view cyber threats as a technical problem, rather than an issue that requires board-level attention.

Mr Huggins agrees. He believes asset managers have tended to focus on low-level

Fidelity Investments joined a list of 13 financial institutions attacked by hackers last summer. The attack was believed to be related to the breach suffered by JPMorgan, the US investment bank, which potentially exposed the names, addresses, telephone numbers and emails of 76m households.

In-house trading algorithms, the life blood of quantitative hedge funds and high-frequency traders, are also being targeted by cyber criminals wanting to sell them on to unscrupulous traders. Security experts say there has been a spate of targeted attacks aimed at stealing the code that underlies trading strategies, as hack-

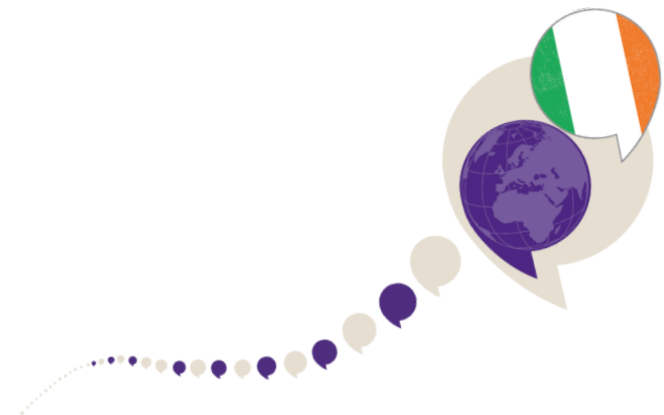
ers home in on financial companies' intellectual property.

Security company Kroll has observed three recent cases, Ernest Hilbert, head of cyber investigations for Europe, the Middle East and Africa, told FTfm in February. "We have seen cases of the source code for algorithms being stolen. In two of the cases we were able to

find the bad guy and stop him before he could share it on the web," he said.

The Central Bank of Ireland's on-site inspections are expected to be finished by the end of June.

*Attracta Mooney is a senior reporter on Ignites Europe, an FT news service*



# What is the problem



# Increasing issues

ft.com > markets > ftfm >

## Regulation & Governance

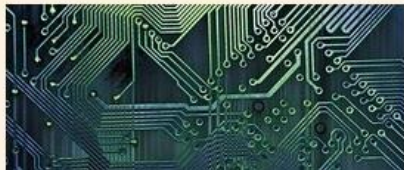
Home World ▾ Companies ▾ Markets Global Economy ▾ Lex ▾  
fastFT Alphaville FTfm Markets Data ▾ Trading Room ▾ Equities ▾ Currencies Capital Mk

February 22, 2015 6:39 am

### Cyber criminals target trading algorithms

Judith Evans

Share ▾ Author alerts ▾ Print Clip Comments



In-house  
of quan  
frequen  
cyber c  
unscrup

**USA TODAY**  
A GANNETT COMPANY

Search  **SU** to g

NEWS SPORTS LIFE **MONEY** TECH TRAVEL OPINION 71° CROSSWORDS MORE

### DOJ: Cyber extortionists targeting hedge funds

 Kaja Whitehouse, USAToday 4:36 p.m. EDT May 8, 2015

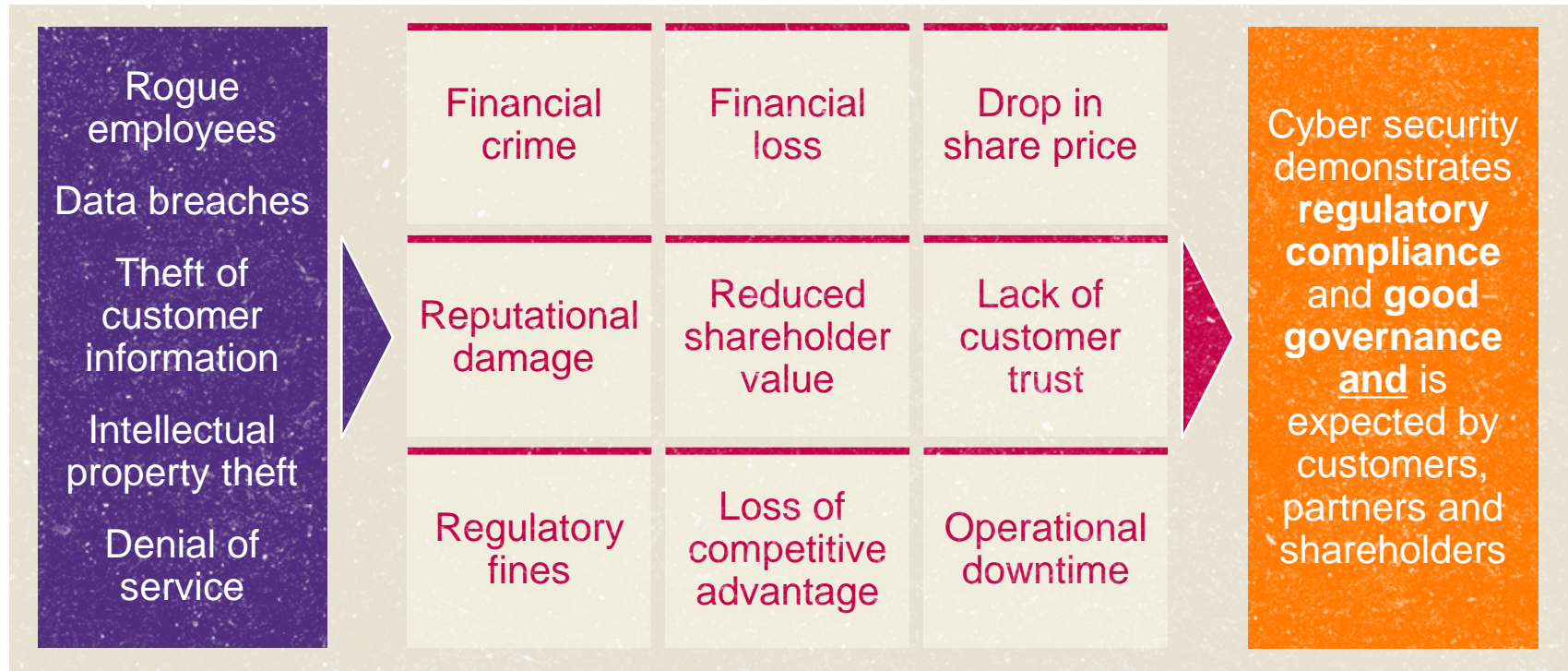
 **The Interview**  
From \$5.99  
Rated: R  
Released: 2014  
Running time: 1  
Language: English  
CC



LAS VEGAS – The government is working with "several" hedge funds that have been victims of cyber extortionists, said John Carlin, head of the Justice Department's National Security Division.

**TOP VIDEO**  


# Impact



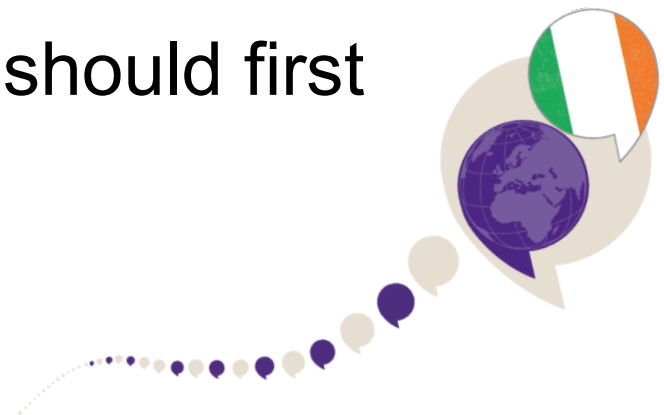


# Sutton's Law



William F. "Willie" Sutton

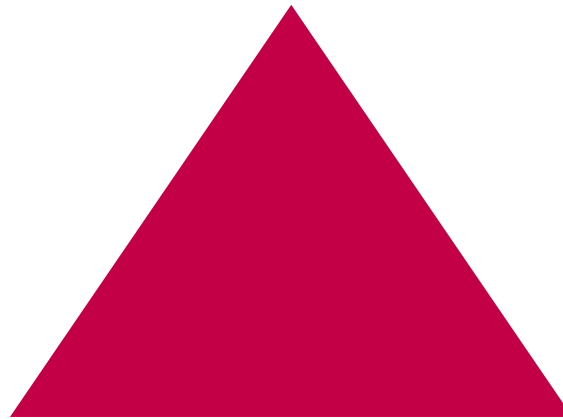
“When diagnosing a problem, one should first consider the obvious”





# Cressey's fraud triangle

Motivation



Opportunity

Rationalisation

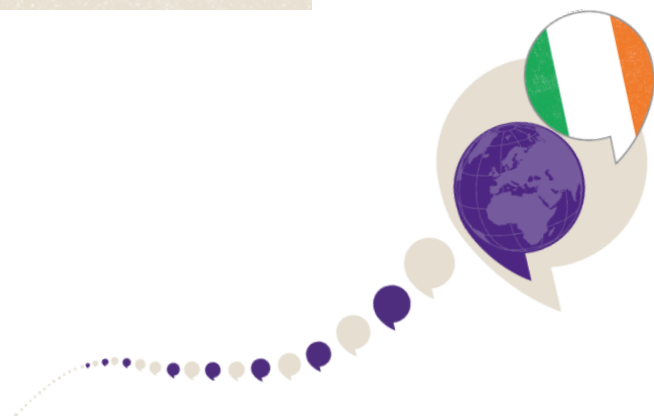
Opportunity = knowledge + privilege + liberty



# What is Cybersecurity

Cybersecurity is the **ability**  
**to protect or defend** an  
organisation's online systems  
and technology from attack

$$R = T \times V \times C$$



# The bad guys have changed...



*10 years ago,  
they looked  
like this...*

...radically



*"Do you think now that we're doing fewer illegal things  
we can scale back the legal department?"*

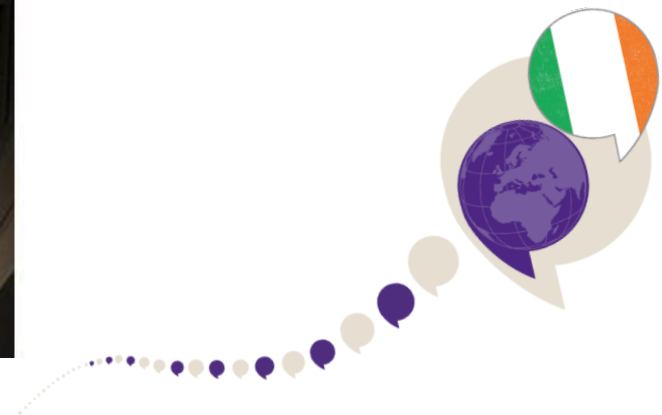
*Now they  
look like  
this...*

# Carbanak – *the biggest bank heist ever*

## The greatest heist of the century: hackers stole \$1 bln

February 16, 2015 Alex Drozhzhin Featured Post, Malware, News, Security, Threats

Advanced Persistent Threats, or APTs, are a pet subject for infosec experts to talk about, as such attacks usually employ the most sophisticated hacker tools. However, for common folks such threats are of no interest whatsoever.





# Denial of service for cash



# DD4BC – the professionals



*Improving the cyber security posture of New Zealand*

Home

Membership

Events

News

Contact

'Pay bitcoins or your network gets it' threats for New Zealand organisations.

Members Trust Portal



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team

Homepage | Contact

English

GovCERT.ch Blog

Whitepapers

Report an Incident

Statistics

GovCERT.ch Blog

## Increase in DDoS extortion (DD4BC)

Published on 2015-05-08 11:00:00 UTC by GovCERT.ch ([permalink](#))  
Last updated on 2015-05-08 11:05:59 UTC

In the past days MELANI / GovCERT.ch has received several requests regarding a Distributed Denial of Service (DDoS) extortion campaign related to 'DD4BC'. The *DD4BC Team* (that is how the attackers call themselves) started its DDoS extortion campaigns in [2014](#). While these attacks

GovCERT.ch Blog

- [Blog RSS feed](#)
- [Blog Index](#)

Social Networks

- [Follow GovCERT.ch on Twitter](#)



Hello,

To introduce ourselves first:

<https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html>

<http://bitcoinbountyhunter.com/bitalo.html>

<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>

Or just google "DD4BC" and you will find more info.

Recently, we were DDoS-ing Neteller. You probably know it already.

So, it's your turn!

[<site>](#) is going under attack unless you pay 20 Bitcoin.

Pay to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack on your server.  
Don't worry, it will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 20 BTC at the moment, so we are giving you 48 hours to get it and pay us.

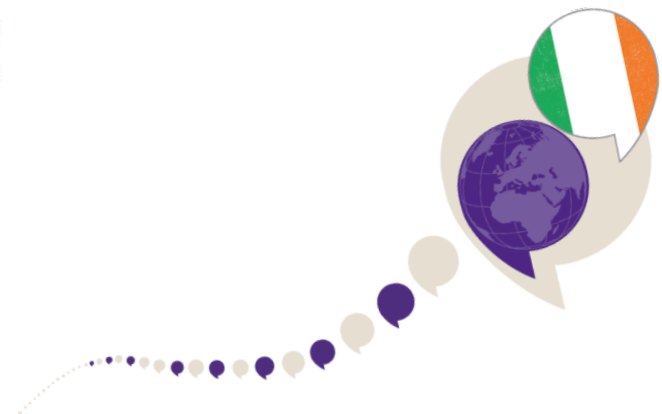
We do not know your exact location, so it's hard to recommend any Bitcoin exchanger, so use Google.

Current price of 1 BTC is about 250 USD.

IMPORTANT: You don't even have to reply. Just pay 20 BTC to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z – we will know it's you and you will never hear from us again.  
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service.

But if you ignore us, and don't pay within 48 hours, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

ONE MORE TIME: It's a one-time payment. Pay and you will not hear from us ever again!



# Irish financial services organisation targeted

1

**Day 1 2:00PM:**  
**Received email**  
from DD4BC  
seeking €6,000 in  
24 hours to avoid  
systems outage

2

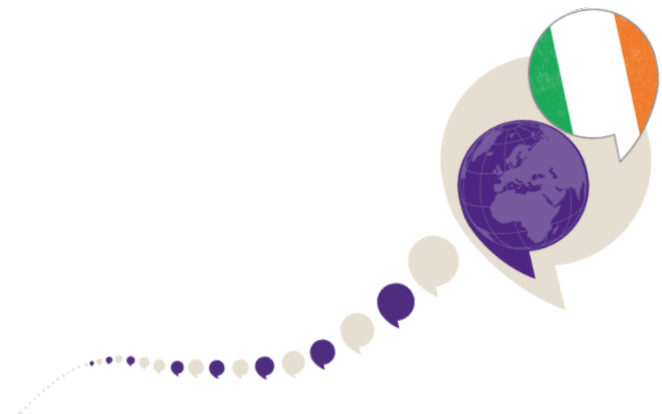
**Day 1 4:00PM:**  
**Systems offline**  
after large flood of  
traffic. Attack stops  
after 5 minutes.

3

**Day 1 6:00PM:**  
**Datacentre**  
provider says it will  
take 3 days to put  
defences in place

4

**Day 2 2:00PM:**  
**Further email**  
from DD4BC  
extending deadline  
by 24 hours



Hide Your IP address If you are going to DDOS others, above is the Cheapest VPN I can find. This will block incoming DDos attacks, protect your own connection, and keep you anonymous Online

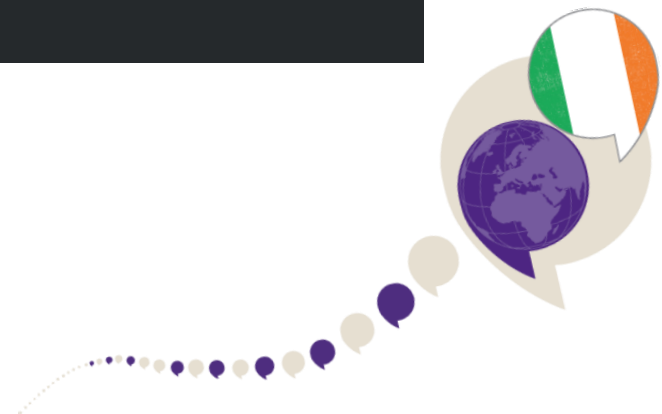
- Free Skype Beta Resolver - <http://www.iSkypeResolve.com>  
- Make Thousands of Dollars Online - <https://www.cpagrip.com>

## Top 10 Booters

- #1: Network Stresser - <http://Networkstresser.com> (120GB/seconds)(Skype Resolver)(Stop Button)(Strongest Ever)(Admin's Choice)
- #2: PowerStresser- <http://powerstresser.com> (80GB/seconds)(Skype Resolver)(Good Staff)(Powerful)(Accepts Credit Cards)
- #3: EchoStress- <http://echostresser.com> (Max Time)(Best for Xbox)(Very Powerful)(Skype Resolver)
- #4: FinitBoot- <http://finitboot.com> (Very Powerful)(Best for Xbox)(Max Time)(Cheap)
- #5: ExoStress- <http://exostress.in> (Strong Power)(Up For 4 Years)(Easy Site)
- #6: Layer4- <http://layer-4.com> (Decent Power)(Friendly Staff)
- #7: IP Stress Test - <http://ipstresstest.com> (Max Time)
- #8: Legion Booter - <http://legion.cm> (Strong)
- #9: IDDoS Stresser - <http://iddos.net> (Hard Hitting)
- #10: Avenge Stresser - [www.avengestresser.com/](http://www.avengestresser.com/) (Great Price)

## How Do I use It?

Register and Log In!!





# Cyber extortion in Irish banking

**YOUR COMPUTER HAS BEEN LOCKED!**

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:  
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

**CryptoLocker**

**Your Personal files are encrypted**

Your personal files **encryption** produced on this computer: photos, documents, etc. Encryption was produced using a **unique** public key generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, is on a secret server on the Internet; the server will **destroy** the key specified in this window. After that, **nobody and never will be able** to decrypt your files...

To **obtain** the private key for this computer, which will automatically decrypt your files, you need to pay **1.00 bitcoin** (~299 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin". To open a list of encoded files, click "Show files".

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on  
1/6/2015 12:53:45 PM

Time left  
**71:53:30**

Checking wallet.  
Received: **0.00 BTC**

Show files Pay with Bitcoin

**CryptoLocker**

**Payment for private key**

Choose a convenient payment method:  
Bitcoin

**bitcoin**

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address  
**1KP72fBmh3XBRfuJDMn53APaqM6MRspCh** and specify the transaction ID, which will be verified and confirmed.

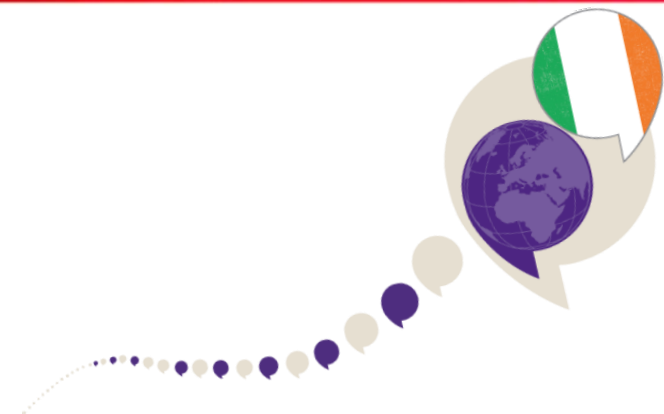
[Home Page](#)  
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

Time left  
**71:55:23**

Bitcoin payment

<< Back PAY



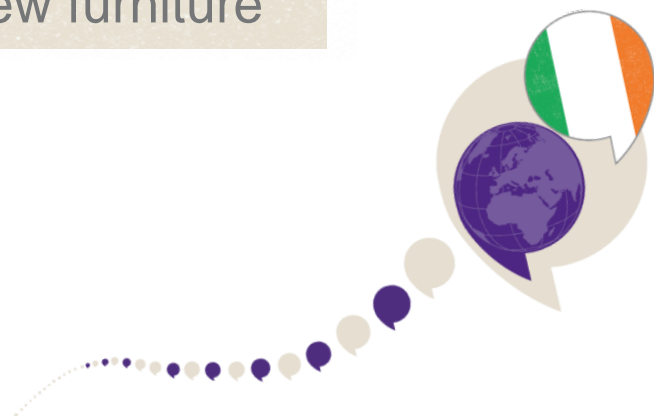
# Cyber extortion in Irish banking

## The issue:

- large amount of data unavailable
- no malware alerts
- scramble to restore files
- no idea how it happened

## The response:

- forensic investigation
- malware identified as cryptolocker.E
- Anti virus did not identify it until 4 days after attack
- call centre staff member had clicked link while surfing for new furniture



# Customer attacks in banking

## Malware based:

- emails from known individuals
- forwarded from CFO to controller
- €900,000 transferred in 8 hours

## Social engineering:

- grooming of finance staff
- 8-9 month lead time
- helpful demeanour
- £600,000 in one incident in Northern Ireland



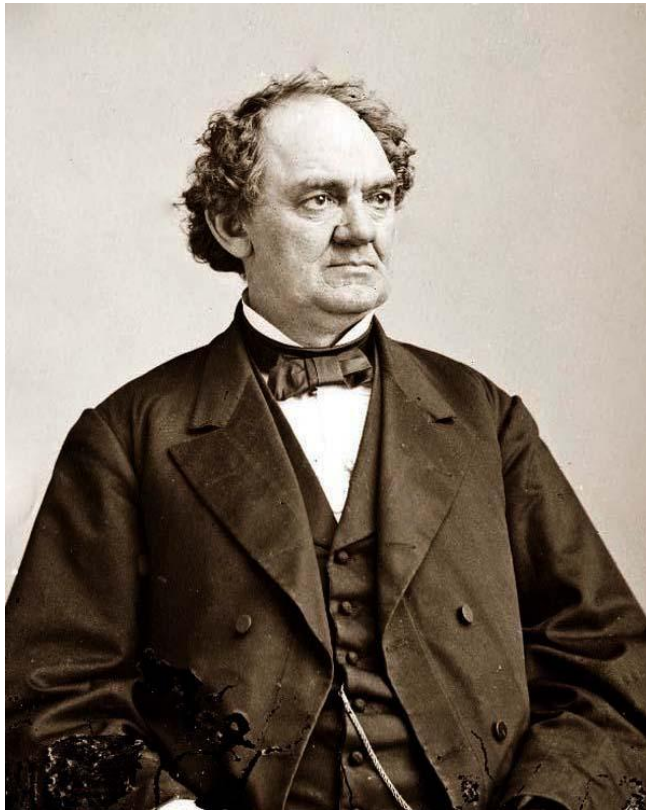
*Corporate customers increasingly aggressive in recovery*



# Social engineering...

“There’s a sucker born every minute”

Phineas T. Barnum



# Phishing etc.

Phishing  
Pharming  
Vishing  
Spear Phishing  
Trojan Phishing  
Baiting





# “Old fashioned” credit card theft

## Gardai focus on eastern Europe in credit card fraud investigation



Maeve Sheehan

PUBLISHED

17/11/2013 | 01:00



SHARE

THE GARDA fraud squad has joined international police forces in trying to track down the gang that stole credit card and bank details of tens of thousands of Irish people.

### [Earn €75 Per Week Online](#)

Companies Pay You For Your Opinions It's Easy, Free & Fun. Earn Now!  
[surveycompare.net](http://surveycompare.net)

### [Watch Full Episodes](#)

Turn Your Computer into a TV! Watch with TelevisionFanatic™ Now  
[www.televisionfanatic.com](http://www.televisionfanatic.com)

Ads by Google

Detectives investigating the audacious theft of personal details of customers began making inquiries through Interpol and Europol's dedicated cyber crime unit following one of the biggest personal security breaches in the history of the State.

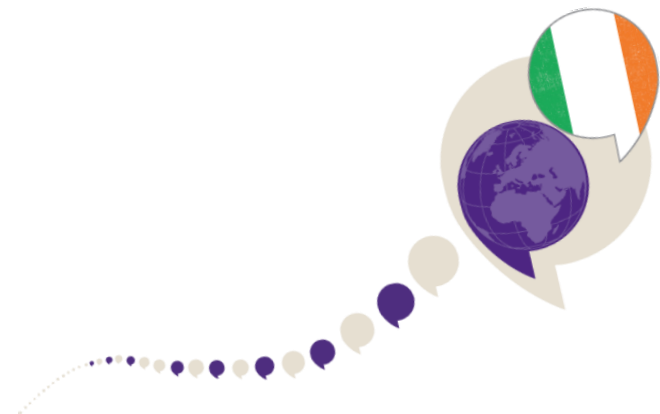
Suspicion is now centring on eastern European cyber hackers, as investigators focus inquiries abroad.

Informed sources revealed that the hacking is believed to have occurred on October 18 when hackers broke into the database of a marketing firm, Loyaltybuild in Co Clare.

The crime was not detected until October 25, giving ample time for the criminals to make use of the 376,000 credit card details stolen from the database.

News of the breach broke only last week, when the firm, Loyaltybuild, which is based in Ennis, Co Clare, confirmed that it had been targeted in what it called a sophisticated criminal attack.

Loyaltybuild runs loyalty holiday deals for customers of some of Ireland's biggest retailers and insurers.



CC

[Bulk Orders - Low Prices!](#)

Country	CC type	CC mark	Debit/Credit
All <a href="#">All USA</a>	All <a href="#">All Visa</a> <a href="#">Master</a>	All <a href="#">All Gold</a> <a href="#">Platinum</a>	<input checked="" type="checkbox"/> DEBIT <input checked="" type="checkbox"/> CREDIT
Zips & Bins	Bank & State & City	Base	Additional
<div>91111, HJ4111</div> <div>380282, 376282</div>	Bank: All State: All City: All	All	<input type="checkbox"/> Expiring 09/14 <input type="checkbox"/> Phone <input type="checkbox"/> VBV <div>Exp. date (1312)</div>

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#)

Clear

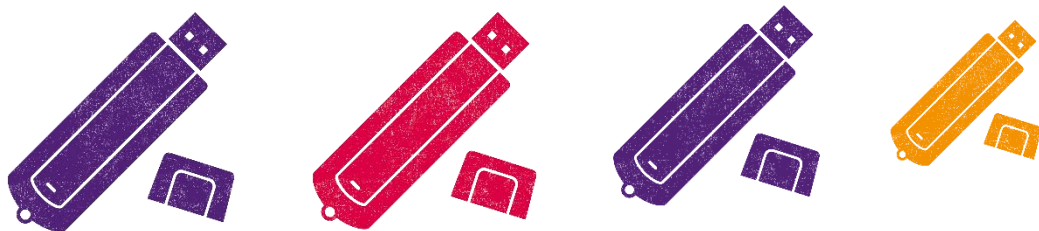
Search

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expires	Country	Sate	City	Zip	Phone	VBV	Base	Price	Cart
<input type="checkbox"/>	601149	 DISCOVER	CREDIT	CONSUMER PREMIUM CAR	03/2019	 United States	TX	Houston	77084			Vetranko-S 	7.5\$	<input data-bbox="1574 811 1632 846" type="button" value="+"/>
		Dump or cc of this particular bank (BIN) cannot be replaced or refunded.												
<input type="checkbox"/>	526225	 MASTERCARD CITIBANK N.A.		STANDARD	11/2016	 United States	CA	Riverside	92504	Yes		Vetranko-S 	7.5\$	<input data-bbox="1574 932 1632 968" type="button" value="+"/>
		Dump or cc of this particular bank (BIN) cannot be replaced or refunded.												

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845		Charles A B	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
528713		Christopher B	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
645450		C MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
371527		C MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
646880		DAVID MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
651920		DAVID J	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
645857		D MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
371198		D MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
534248		DAVID M	US	LA BETH	Y	Y	Y	40\$	<input type="checkbox"/>
371726		DAVID M	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
537161		DAVID M	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
447639		DAVID M	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
371730		D MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
528730		D MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
653659		D MICHAEL	US	LA BETH	Y	N	Y	40\$	<input type="checkbox"/>
									<input type="button" value="Buy"/>

# Simple data theft:

## *Typical scenario*

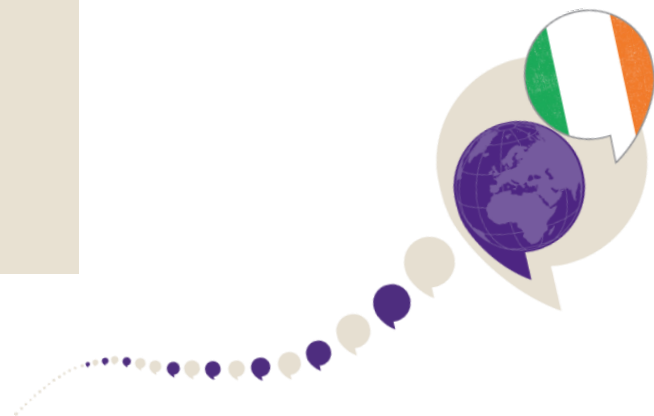


Member of staff obtains a job with a competitor / organisation in the same sector

Copies data accessible to them onto a USB Pen / web-mails via Gmail / copies it to Dropbox etc.

Does something stupid so the theft is detected.

**Motivation? – Stupidity, Greed, Anger.**



# Data theft

- **USB “pen” or “thumb” drive**
- **portable hard drive.**
- **MP3 Players, digital cameras, Memory cards, PDAs**
- **CD/DVD.**
- **E-mail**
- **Web-mail**
- **printing**
- **remote access.**





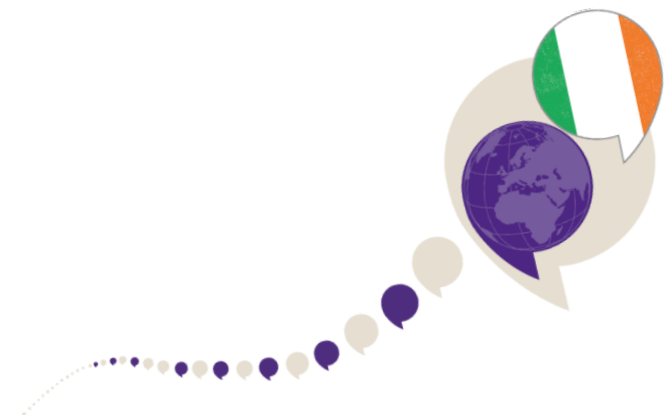
# Data theft risk factors

- sudden resignation/departure of staff
- departure of staff to commercial competitors
- departure of staff to start their own business or other enterprises
- staff with access to sensitive data involved in disciplinary or relationship issues
- staff leaving under redundancy
- staff in personal relationships with persons in competing organisations
- staff in personal relationships with journalists
- companies undergoing financial or industrial relations problems.

# Hacking – there's nothing like advertising!



The screenshot shows the Fox News website interface. At the top is the 'FOX NEWS' logo and a search bar. Below the logo is a navigation menu with links: Home, Gadgets, Google, Social, Military Tech, Smartphones, Video Games, and Slideshows. A large banner advertisement at the top reads 'That's why we give you up to 10 months' mortgage approval'. The main headline is 'Xbox Live back online, PlayStation Network still down after apparent hack attack', with the category 'HACKERS' above it. Below the headline, it says 'Published December 26, 2014 · FoxNews.com' and shows social media share counts for Facebook (655), Twitter (1288), and Google+ (2224). There are also icons for email and printing. Below the article text is a video player showing two boys playing video games, with the title 'HACK ATTACK' and 'Gaming systems the target of hack attack?'. To the right of the video player is a section titled 'More from Fox News' with a red curtain background.



# Political hacking

## THE WALL STREET JOURNAL

Home World U.S. Politics Economy **Business** Tech Markets Opinion Arts Life Real Estate

Subscribe Now | Sign In  
**€12 FOR 12 WEEKS**

Search



Fiat Chrysler  
Faces \$105 Million  
Fine for Recall  
Lapses



Teva in Talks to  
Buy Allergan Unit in  
\$45 Billion Deal



Chinese Firm  
Plans \$5 Billion Fund  
for Overseas Tech  
Acquisitions



More Layoffs  
Expected at U.S.  
Energy Firms



Palm  
BlackBerry  
Due to 5  
Concerns

**YOU ARE READING A PREVIEW OF A PAID ARTICLE. SUBSCRIBE NOW TO GET MORE GREAT CONTENT.**

BUSINESS

### Anthem: Hacked Database Included 78.8 Million People

Health insurer says data breach affected up to 70 million Anthem members



Home Cyber Crime **Cyber warfare** Digital ID **Hacking** Intelligence Laws  
Mobile **Security** Social Networks Reports SA Team EXTENDED COOKIE POLICY



Hackers hit South Korea also spread spyware to steal military secrets





# Personal data theft

## CVSphoto.com

We have been made aware that customer credit card information collected by the independent vendor who manages and hosts CVSPhoto.com may have been compromised. As a precaution, as our investigation is underway we are temporarily shutting down access to online and related mobile photo services. We apologize for the inconvenience.

Customer registrations related to online photo processing and CVSPhoto.com are completely separate from CVS.com and our pharmacies. Financial transactions on CVS.com and in-store are not affected.

Nothing is more central to us than protecting the privacy and security of our customer information, including financial information. We are working closely with the vendor and our financial partners and will share updates as we know more.

For more information, call 1-800-SHOP-CVS.

Members Login ▾

# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▾

**See Your Matches »**

Over **38,085,000** anonymous members!

★★★★★  
**100%**  
Like-minded  
People

**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim

Ashley Madison is the world's leading married dating service for *discreet* encounters

 Trusted Security Award

 100% DISCREET SERVICE

 SSL Secure Site

Register on Ashley Madison | Affiliate Program | Press | FAQ | Guarantee | Blog | Infidelity News | Articles | Terms | Privacy | Contact Us

Follow Ashley Madison on: [Twitter](#) | [Facebook](#) | [Youtube](#)

Location: [Ireland](#) ▾ | Language: [English](#) ▾

## 650,000 Paddy Power customers had data stolen in 2010 breach

22 29 + ↻

Thursday 31 July 2014 17.42



Customers who held accounts since 2010 or earlier have been affected by the breach

The office of the Data Protection Commissioner has said it is disappointed that Paddy Power failed to report a major data security breach that occurred in 2010.

In a statement this afternoon, it said the breach should have been reported in line with best practice.

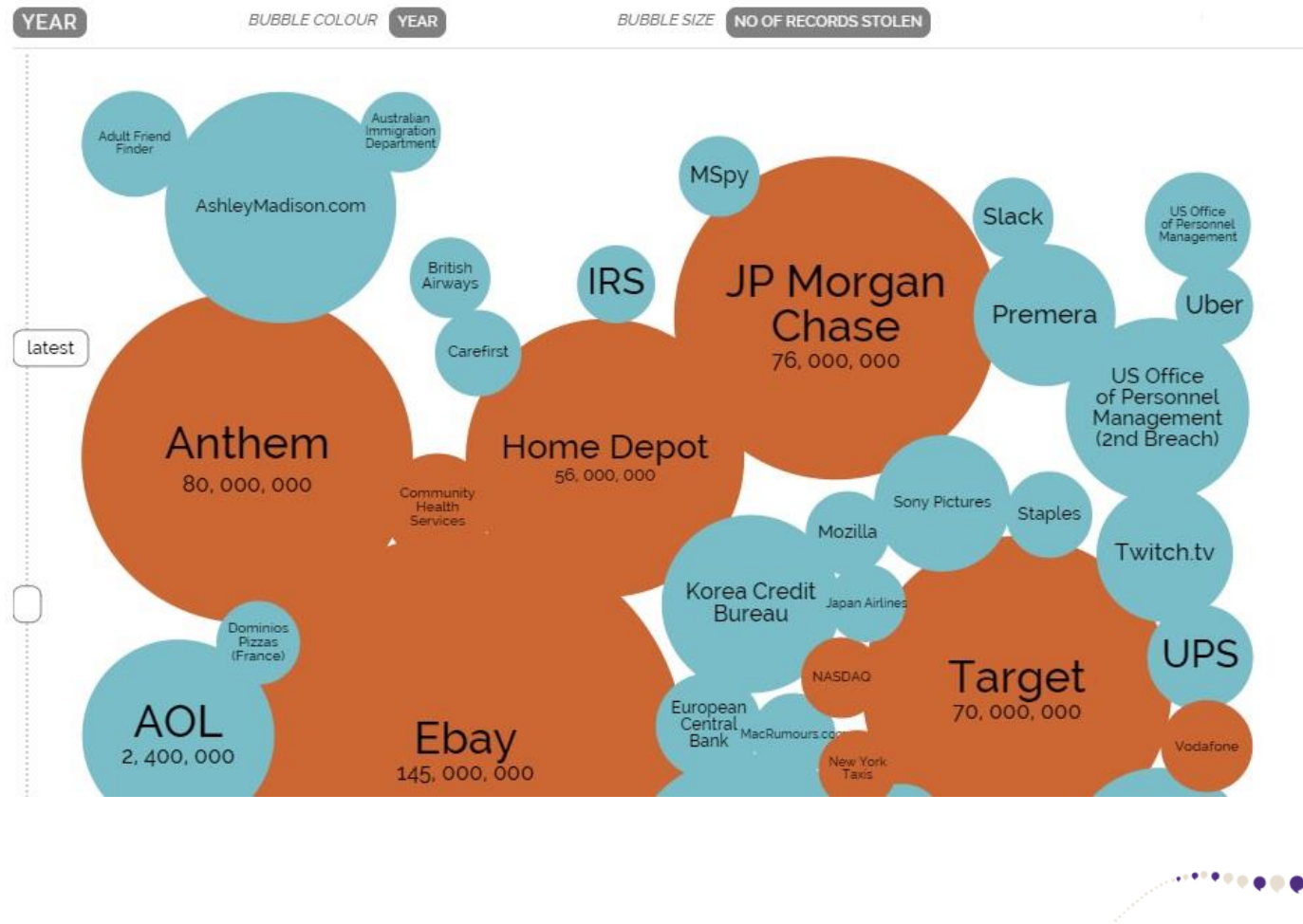
It said that an investigation into the incident was continuing and further recommendations from the office to Paddy Power would result.

The incident, in which details relating to more than 600,000 Paddy Power account

# But don't forget....

## World's Biggest Data Breaches

Selected losses greater than 30,000 records





## Go

Categories

Drugs (2762)

Services (1331)

Data (633)

Weapons (210)

Collectables (30)

Metals/Stones (29)

Other (354)

Software (165)

Movies (27)

Tobacco (169)

Counterfeits (248)

Alcohol (11)

eBooks (1667)

Weight Loss (17)

Exchange

Exchange

User Menu

Home

Inbox (0/0)

Account

Purchases

Favorites

Deposit Addresses


Forum

Rates




\$ 125.3900

Weapons > Firearms

( AK-74 BRAND NEW FULL AUTO 5.45x39mm



More images:



Price

19.93779 BTC

\$ 2,500.00 £ 1,554.92 € 1,844.20

Ship from

USA

Ship to

Worldwide

Stock

2

Created in

2013-08-26 02:31 UTC

Last update

2013-09-16 15:29 UTC

Listing Feedback

0/0/0

Your balance isn't enough to buy this item! Please deposit the needed funds before.

Description

For sale is SELECT FIRE AK 74 built from beginning as such. Not a converted semi auto, legit full auto function just like factory rifle. I built the rifle with original UNISSUED Bulgarian AK 74 parts and quality US made barrel and receiver. Headspace checked to ensure safe operation. Because gun was made of brand new parts, some of them still covered in anti-rusting grease.

Bulgarian made polymer stocks.

I can add extra parts and accessories at you cost.

Select fire shoot both semi auto and full auto. Rifle is **BRAND NEW** only 30 rounds fired for test. Include 1 magazine and 30 rounds of 5.45x39mm surplus Russian ammo.

Full escrow.

Shipping Table

Description	Price
US/mexico mild stealth 1-3 days with tracking	0.79751 BTC
Worldwide high stealth 6-10 days with tracking	2.39254 BTC

Questions to Vendor


Question by: Battosai at 2013-09-17 05:07 UTC

Select fire ? can you have ammo ?

Answered by the seller at 2013-09-17 15:28 UTC

yes and yes

Seller Info



User lereyjenkins47

Feedback 3

Reg. Date 2013-07-19 01:16 UTC

Last login 2013-09-19 19:05 UTC

View Profile

Other Listings

Contact seller

Add to Favorites

# So, how bad can it get?



## Technology

### Hack attack causes 'massive damage' at steel works

🕒 22 December 2014 | Technology



A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

#### Top Stories

**Syrian leader**

🕒 2 hours ago

**Turkey calls  
PKK**

🕒 1 minute ago

**Vettel wins c**

🕒 2 hours ago



#### Features





# So, how bad can it get?

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

## AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX



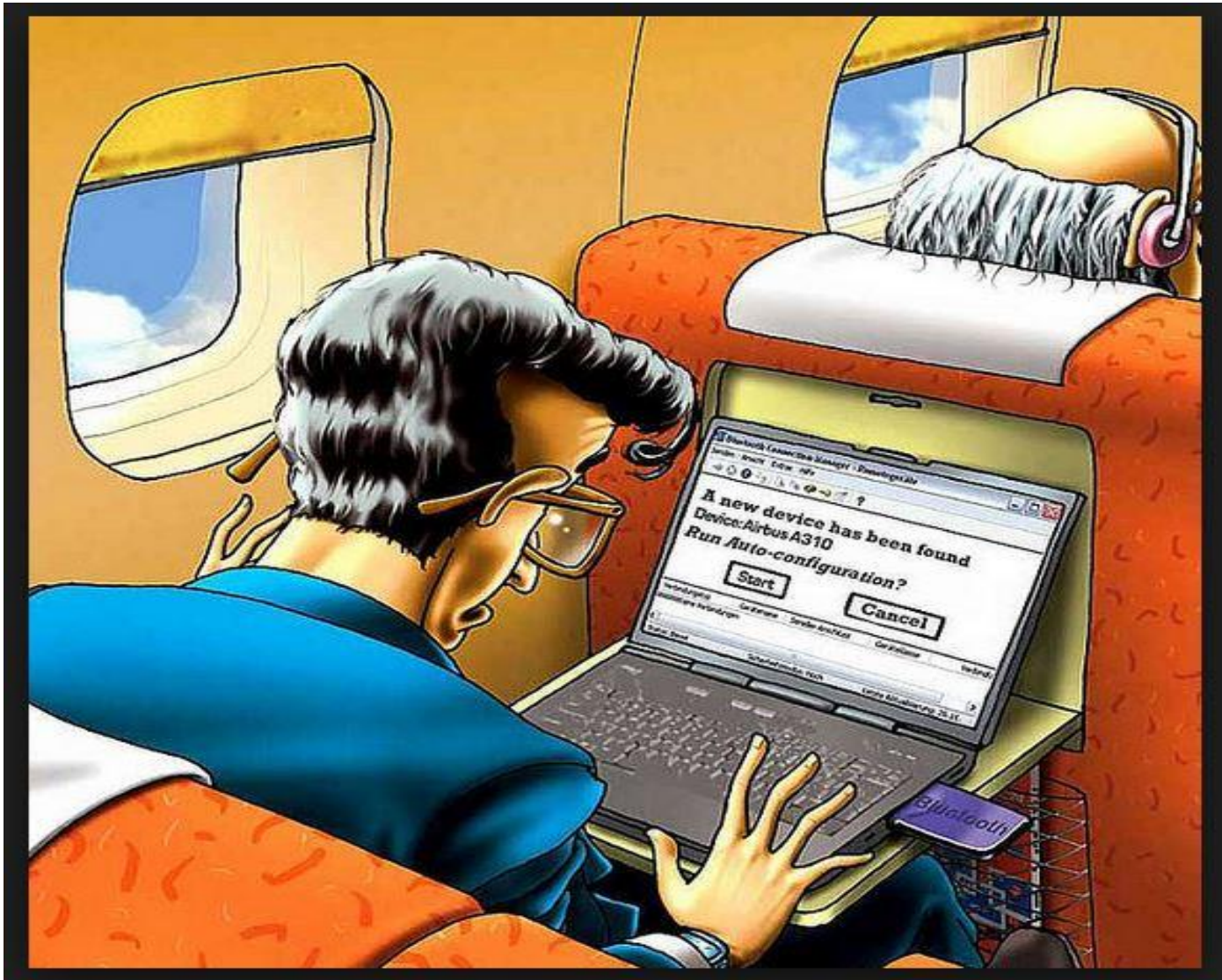
ACTIVELY PROTECT  
YOUR NEW DEVICE  
WITH  
**NORTON™ SECURITY**

ACTIVATE NORTON



LATEST NEWS

# So, how bad can it get?





Search

NEWSSPORTSLIFEMONEYTECHTRAVELOPINIONWEATHERCROSSWORDSYOUR TAKEINVESTIGATIONSVIDEOSTOCKS

18060  
  
951  
  
619  
  
239

# FBI: Computer expert briefly made plane fly sideways

Elizabeth Weise, USATODAY 8:39 p.m. EDT May 16, 2015

CONNECT
   
TWEET
   
LINKEDIN
   
COMMENT
   
EMAIL
   
MORE

SAN FRANCISCO — A computer security expert hacked into a plane's in-flight entertainment system and made it briefly fly sideways by telling one of the engines to go into climb mode.

Chris Roberts of One World Labs in Denver was flying on the plane at the time it turned sideways, according to an FBI search warrant filed in April.

The warrant was first publicized on Friday by [APTN](#), a Canadian News Service.

Roberts told the FBI he had hacked into planes "15 to 20 times," according to court documents first made public Friday.

Roberts first made news in April when he was told he couldn't fly on United Airlines because of tweets he had made about whether he could hack into the flight's onboard computer settings.

**USA TODAY**  
Computer security expert blocked from flight after tweets

The FBI search warrant describes him doing just that.

According to the document, in an interview on Feb. 13, 2015, Roberts told agents he had hacked into in-flight entertainment centers on Boeing 737s, 757s and Airbus A-

TOP VIDEOS

Why did AT&T's cable merge succeed when Comcast's failed?



# How should you respond



# What are the SEC saying?

## Assess:

- information and technology used
- threats and vulnerabilities
- controls and processes
- governance and management



## Develop cyber security strategy:

- access control
- encryption
- data loss prevention
- monitoring
- backups
- incident response plan



## Implement:

- policies
- procedures
- training



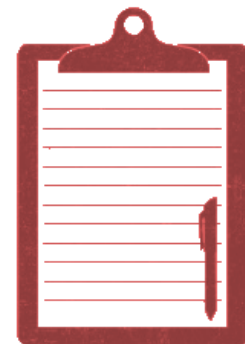
# Central Bank of Ireland themed reviews

## Approach:

- questionnaires
  - on site assessment
- 
- fund managers
  - investment firms
  - stockbrokers
  - banking next

## Focused on:

- risk management
- board awareness & involvement
- cyber policies and procedures
  - access management





# Cyber security areas of concern





# Cyber security organisation focus areas

## Prepare

- Cyber security risk and threat assessment
- Security process or technical assessments
- Security policy development
- Third party cyber security assurance

## Protect

- Security architecture
- Security technology implementation
- Security process design and implementation
- Identity and access management
- Privacy and data protection
- Data classification
- Enterprise application integrity
- Business continuity and disaster recovery
- Penetration testing

## React

- Security operations and monitoring
- Security and data breach incident response

## Change

- Security program strategy and planning
- Security governance
- Security awareness



# Questions & feedback

