paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Cyber Threats – The Threat to CNI

MENA Information Security Conference 2011

Paul C Dwyer – BIO

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Paul C Dwyer is an internationally recognised information security expert with over 21 years experience.

A certified industry professional by the International Information Systems Security Certification Consortium (ISC2) and the Information System Audit & Control Association (ISACA) and recently selected for the IT Governance Expert Panel.

Paul's credentials include:
- -Qualified Hacker
- -SOX (SAS70) Auditor
- -ISO 27001 Lead Auditor
- -BS25999 / BCP Expert
- -Forensic Investigator
- -PCI DSS Specialist
- -Prince2

He has worked and trained with such organisations as the US Secret Service, Scotland Yard, FBI, National Counter Terrorism Security Office (MI5), is approved by the National Crime Faculty and is a member of the High Tech Crime Network (HTCN).

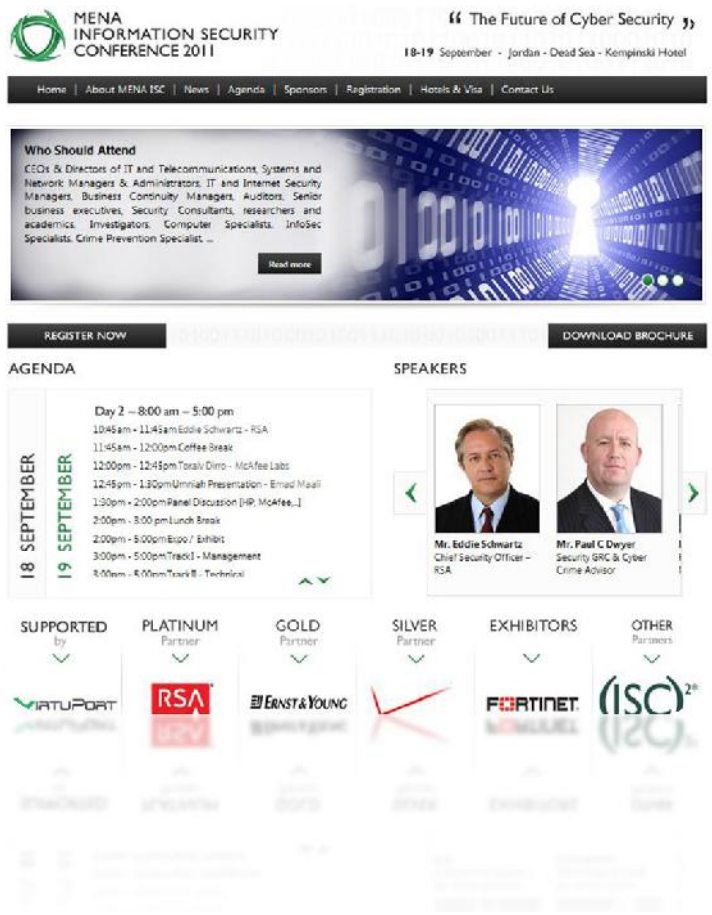
INTERNATIONAL CYBER THREAT TASK FORCE
ICTTF

NACSRO

IRISH CYBER CRIME TASK FORCE

paul C dwyer
Security GRC & Cyber Crime Advisor

NATO
OTAN

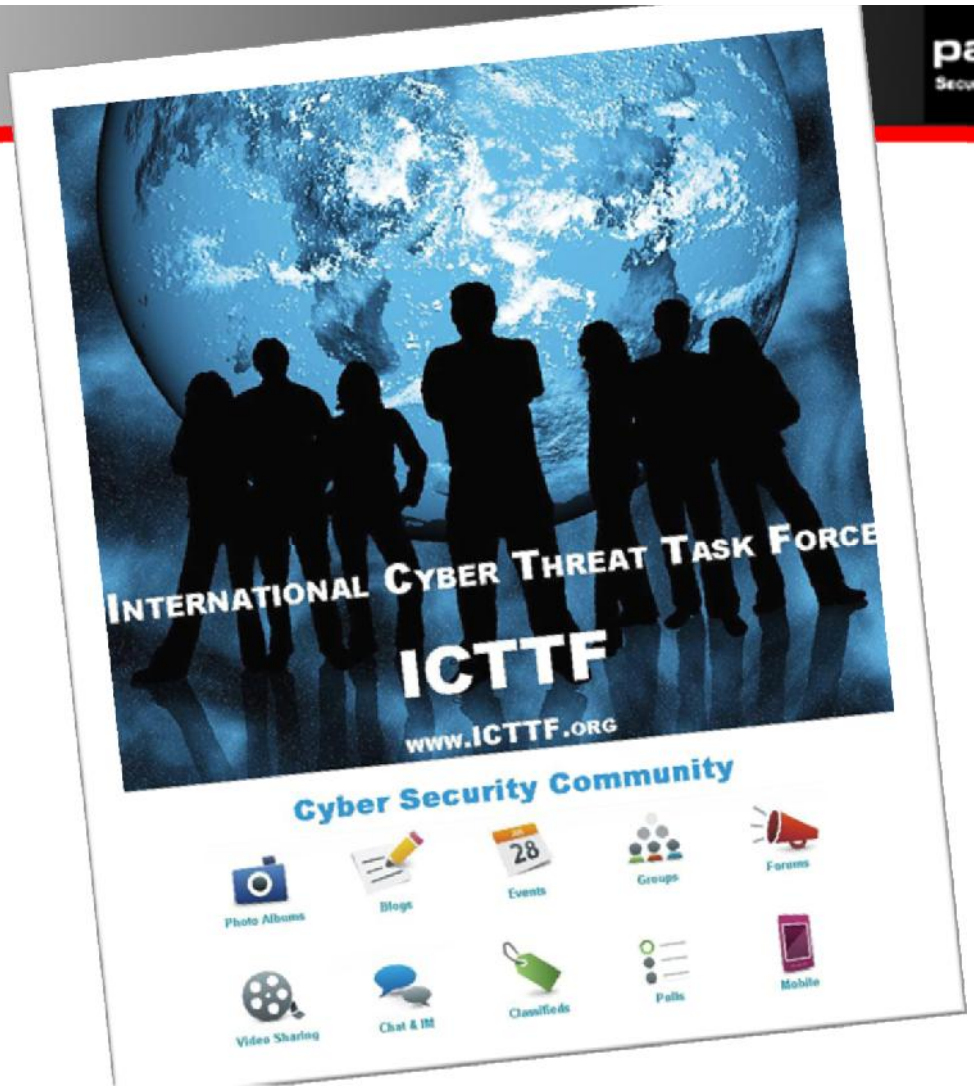


Recap Yesterday

Approach to dealing with
- Risks
- Frameworks
- Security Metrics

ICTTF.org

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS



Cyber Threats - Blurred Lines

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

What is Cyber Crime?

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Cyber crime or computer crime as it is generally known is a form of crime where the Internet or computers are used as a medium or method to commit crime which includes **hacking, copyright infringement, scams, denial of service attacks, web defacement and fraud**.

In our heavily networked world, cyber attacks represent a 24/7/365 threat.

What is Cyber Warfare?

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

- "Digital Infrastructure….Strategic National Asset"
  President Barack Obama
- May 2010 – Pentagon – Cybercom
- UK - a cyber-security "operations centre" (GCHQ)
- "Fifth Domain" The Economist

What is Cyber Scum?

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Paeodophiles
- Stalkers
- Groomers

Critical National Infrastructure

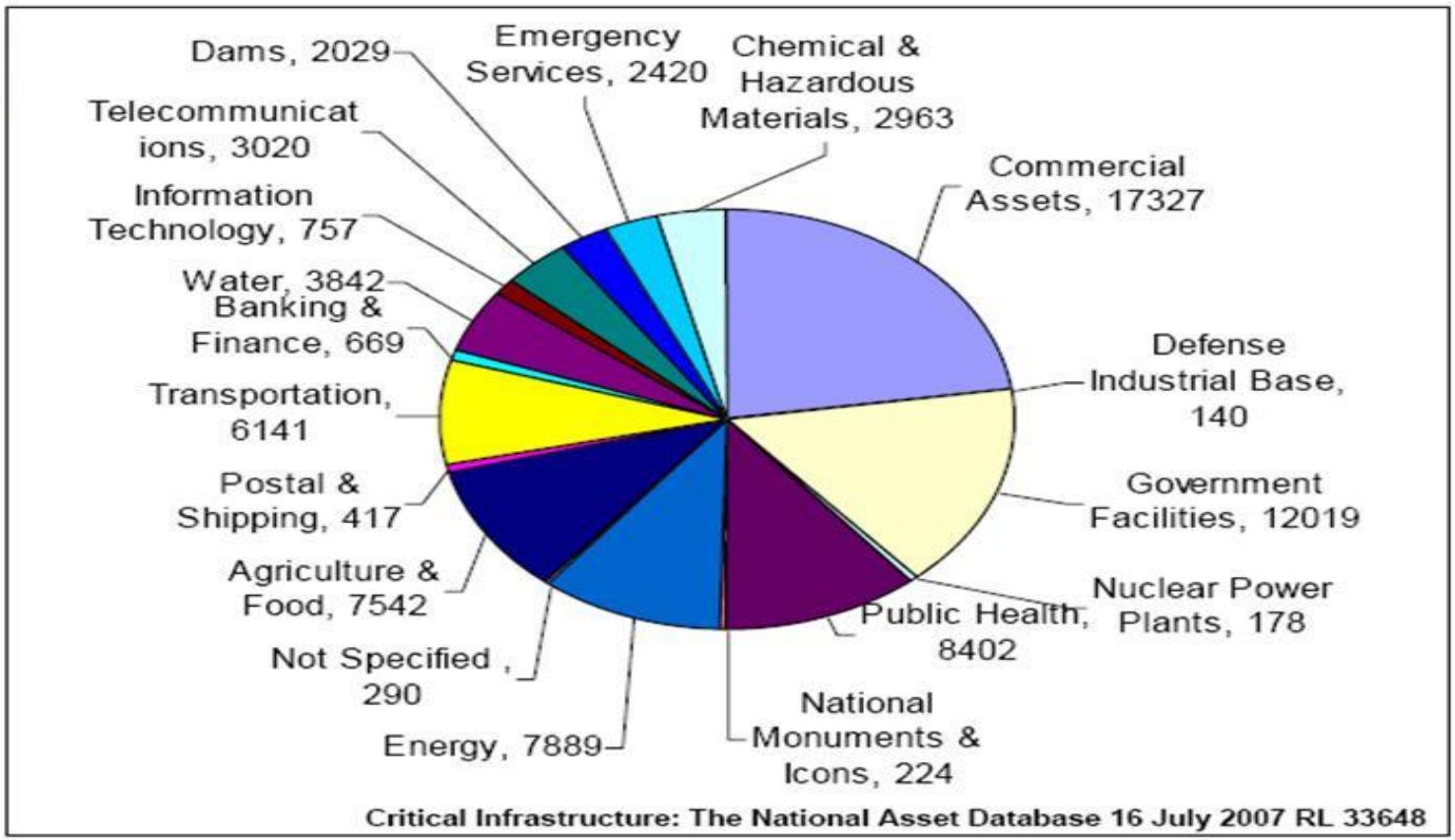
paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Critical infrastructure is a term used by governments to describe assets that are <u>essential for the functioning of a society and economy.</u>

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply drinking water, waste water/sewage, stemming of surface water;
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours);
- financial services (banking, clearing);
- security services (police, military).

National Asset Database Entries by Sector

77,069 assets



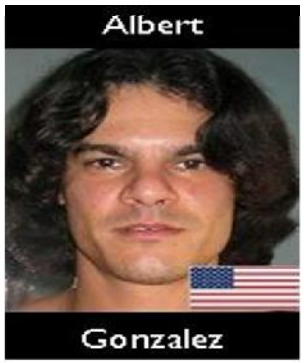
High on Agenda

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

Learn more about our changing world!

“The Daddy” - History

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors



SHADOWCREW
FOR THOSE WHO WISH TO PLAY IN THE SHADOWS

Dark Market

Original Crew

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Turkish LE: 2008

Sectors

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Each sector has its own niches criminals

- Phishers - consumer financial services
- Industrial spies – IP companies
- (H)Activists – social impact they disapprove
- Hackers – scalp for prestige
- Cyber terrorists – hurt for political agenda
- Fraudsters – any to siphon cash

Categories of Attacks

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Criminal Attacks (fraud, theft and grand larceny, identity theft, hacking, extortion, phishing, IPR and copyright theft, piracy, brand theft, 'spoofing')
- Destructive Attacks (cyber-terrorism, hackers, ex-employees, vengeful individuals, cyber war, cyber-vandals, anarchists, viruses)
- Nerd Attacks (Denial of Service attacks, publicity hounds, adware)
- Espionage Attacks (data and IPR theft, spyware)

Threat Groups

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

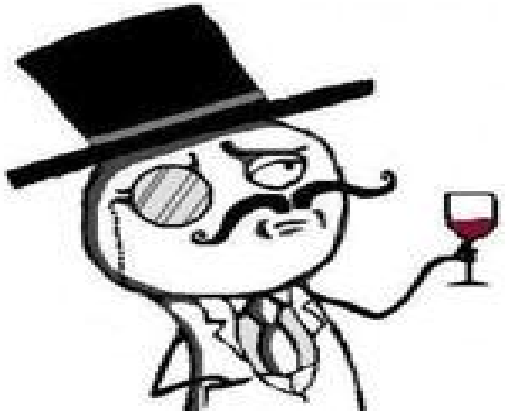
Threats originate with people.

- Criminals (thieves, fraudsters, organised crime)
- Malefactors (hackers, vandals, terrorists, cyber-warriors)
- Spies (commercial and governmental)
- Undesirables (scam artists, spammers,'ethical' hackers)
- The incompetent, or the simply unaware (staff, contractors, customers and other third parties)

These people are found both inside and outside an organisation and can exert an influence out of proportion to their numbers

Hacktivism?

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors



Computer Misuse Legislation

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Computer misuse legislation is relevant in two ways:

- authorities and organisations can take action under it against cyber-criminals

  – organisations have to ensure they comply with it themselves.

  – Directors can be <u>personally accountable</u> for any compliance failures.

Convention on Cyber Crime

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Council of Europe adopted a Convention on Cyber crime that identified and defined internet crimes:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices);
- computer-related offences (computer-related forgery, computer-related fraud)
- content-related offences
- offences related to infringements of copyright and related rights

Directors Responsibility

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- All organisations need to be aware of the Convention's provisions in article 12, paragraph 2: *'ensure that a legal person can be held liable where the lack of supervision or control by a natural person…has made possible the commission of a criminal offence established in accordance with this Convention'.*

- In other words, directors can be responsible for offences committed by their organisation simply because they failed to adequately exercise their duty of care.

Reasons for Escalation

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

It's a business with an excellent economic model.

Other reasons, you name it:

- Technology
- Internet
- Recession
- "A safe crime"
- It's easy to get involved
- Part of Something

Distribute, Wholesale, Resell

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

The most common 'positions' or specializations according to the FBI are:

1. **Programmers.** Who develop the exploits and malware used to commit cyber-crimes.

2. **Distributors.** Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.

3. **Tech experts.** Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.

4. **Hackers.** Who search for and exploit applications, systems and network vulnerabilities.

5. **Fraudsters.** Who create and deploy various social engineering schemes, such as phishing and spam.

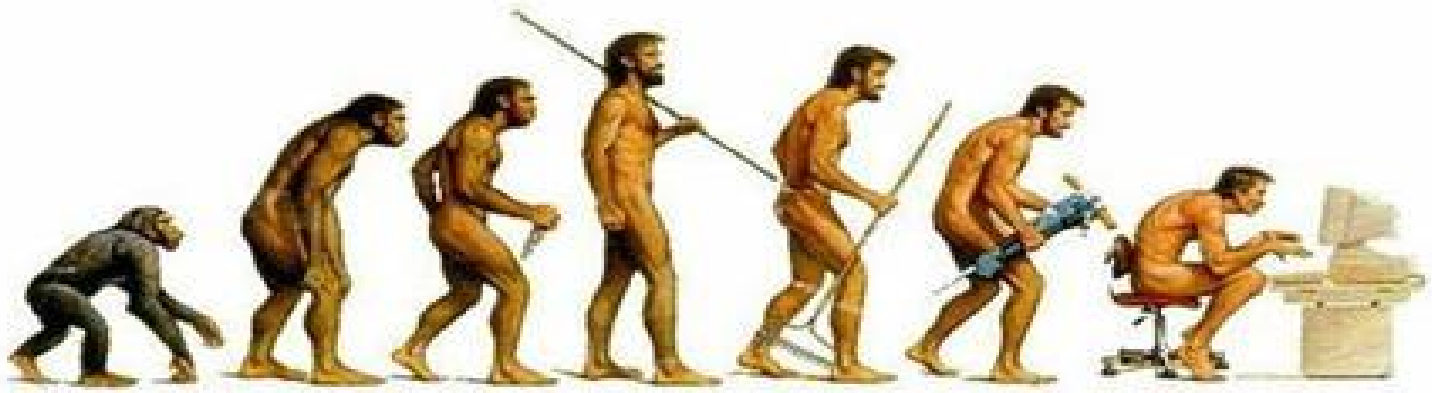
6. **Hosted systems providers.** Who offer safe hosting of illicit content servers and sites.

7. **Cashiers**. Who control drop accounts and provide names and accounts to other criminals for a fee.

8. **Money mules.** Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.

9. **Tellers.** Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.

10. **Organization Leaders**. Often "people persons" without technical skills. The leaders assemble the team and choose the targets.



Malicious Tool Evolution

Crimeware Toolkits

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

Crimeware in the Cloud

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Just-B

PII

Date of Birth:	50.0 Credits
Credit Card Balance:	1.5 Credits
Mother's Maiden Name:	50.0 Credits
Social Security Number:	20.0 Credits
Driver's License Number:	50.0 Credits

PII

5 Credits ~= 1 US Dollar

Example of Crimeware

Tools, Tutorials, Services (Rent & Buy)

Spyeye $500

Botnets (Rent or Own)

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Proxy

Command & Control Server

Infected PC | Infected PC | Infected PC | Infected PC | Infected PC | Infected PC

Spam | Spam | Spam

Website DDoS Attack

Spyeye – Toolkit

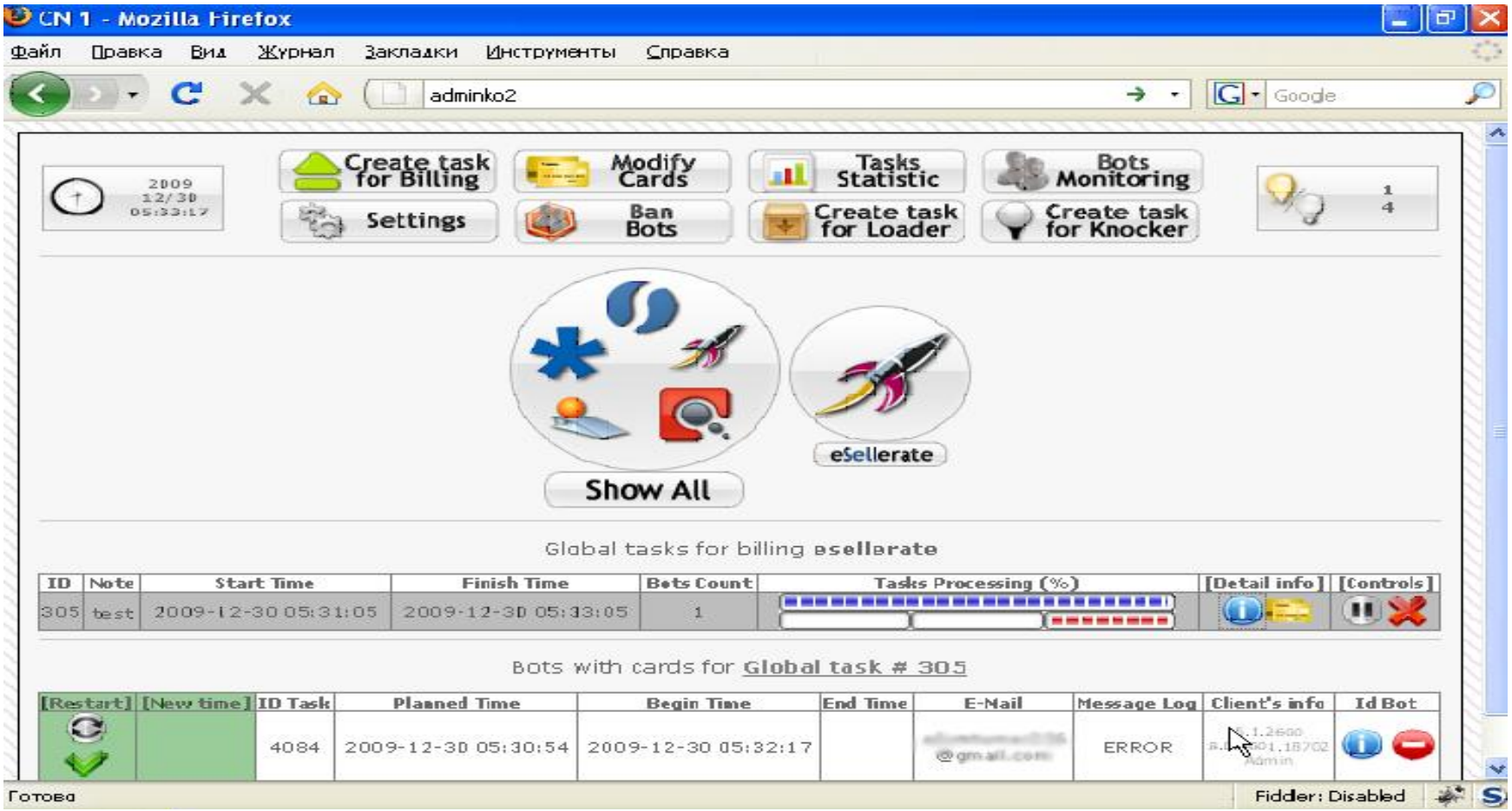
paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Spyeye C & C Server

Install Command and Control



Get CC Info

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Spyeye C & C Server

or Upload List

Infected PC

Infected PC

Infected PC

Infected PC

Infected PC

Infected PC

Place Something For Sale

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Spyeye C & C Server

Uploads, Renames and Claims Ownership of Software Utility For Sale on a popular download store

Automate Transactions

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Spyeye C & C Server

Spyeye automates purchases by form filling at intervals to avoid detection using the stolen credit card information

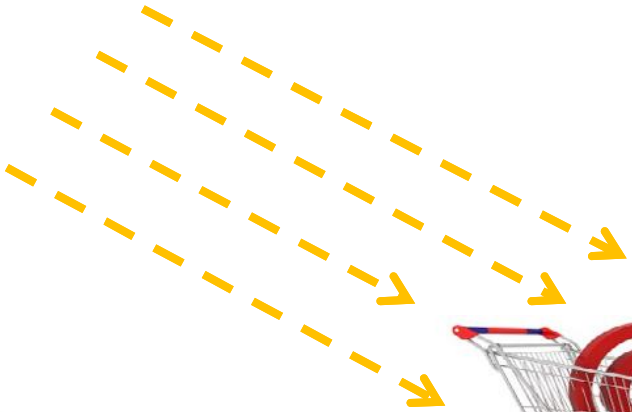
Clean Money

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet
Herder

Proxy

Spyeye C & C Server



Billing Hammer Module

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Avoid Detection

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Botnet Herder

Proxy

Spyeye C & C Server

Billing hammer will send the transaction through an infected machine close to the cardholders address to avoid detection

Cyber Warfare

Is it Real?

Cyber Arms Race

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Oct 2010 Raised $29 Million – “Cloud based Malware and Botnet detection service
- Founders ex IBM ISS and CIA
- Feb 2011 Partnered with Major ICT Vendors
- Anonymous attack on HBGary – leaked info

“provides offensive and defensive vulnerability research”

promises "to provide our customers with the highest quality offensive CNA/CNE (Computer Network Attack/Computer Network Exploitation) software in the world“

Sale of Zero day exploits

Products and Services

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Brokers for Zero day Exploits
- Demo – maps of airports, parliament buildings and corporations
- “Target Packs” by region, Europe, Middle East - Cost $2m
- Submission to Zero Day Exploit Service (25 per year) - $2.5m
- Database of hundreds of millions of infected systems for $1.5m

$6m = Cyber Terrorist

Follow the money…..copycat firms

Measure the problem

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- Cybercrime costs £27 billion a year in the UK
- £1,000 a second

- 170,000 ID's are stolen each year – 1 every three seconds
- Theft of IP £9.2 billion (pharmaceuticals, biotechnology, electronics, IT and chemicals)

- Industrial Espionage £7.6 billion
- Citizens £3.1 billion
- Government £2.2 billion

The £27bn cost of cyber crime

UK Response

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

"the answer lies in private firms and the Government working together to disrupt criminal networks rather than prosecution"

- Cyber attacks on the UK's information technology systems were identified in last year's Strategic Defence and Security Review (SDSR) as **one of the four most serious threats to national security**, alongside terrorism, natural disasters and major accidents.
- Backed by £650 million in new Government funding announced in the SDSR, the National Cyber Security Programme will develop means of responding to threats from states, criminals and terrorists.

Security Minister
Baroness Neville-Jones

UK CNI

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

- Prime Minister David Cameron recently met representatives of some of Britain's biggest private companies to work with the Government on protecting the country against cyber attack.

- Foreign Secretary William Hague and Baroness Neville-Jones also took part in the talks at 10 Downing Street with firms including British Airways, Centrica, the National Grid, BT, Barclays, HSBC and GSK.

- They agreed to form a working party to look at detailed proposals for action, drawing on expertise from the private sector.

NATO

What is mainstream now?

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

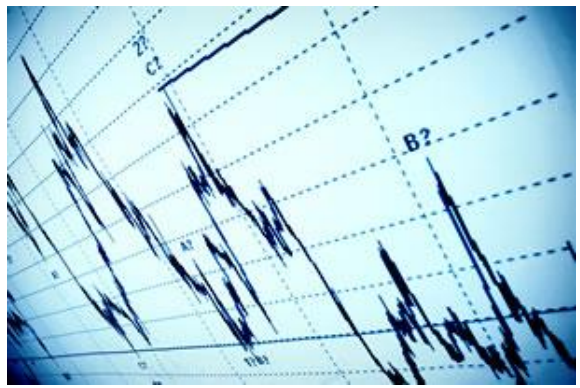
- Social Network / Media Crime
- DDoS
- Child Exploitation Material
- PABX Fraud
- RandsomWare
- Trojans/Malware
- Identity Theft

Type of Service or Product	Description	Average Price (USD)
US Dumps Track1	USA, Name, Account Number, Expiration Date, CW	8
US Dumps Gold Track1	USA, Name, Account Number, Expiration Date, CW	20
US Dumps Discover Track1	USA, Name, Account Number, Expiration Date, CW	8
EU Dumps Tra[illegible]	European, Name, Account Number, Expiration Date, CW	50
EU Dumps Gold Track1	European, Name, Account Number, Expiration Date, CW	90
AP Dumps Track1	Asian/Pacific, Name, Account Number, Expiration Date, CW	40
AP Dumps Gold Track1	Asian/Pacific, Name, Account Number, Expiration Date, CW	50
CD Dumps Track1	Canadian, Name, Account Number, Expiration Date, CW	10
CD Dumps Gold Track1	Canadian, Name, Account Number, Expiration Date, CW	25
Plastics Embossed	Counterfeit Credit Cards with Embossing on card	50
Plastic Banks	Counterfeit Credit Cards	40
Plastics w/ Halo	Counterfeit Credit Cards with security holograms	75
COBs	Change of Billing Information	60
Holos	Holograms	5
Full Infos	Track 1 info plus email address, DOB, MMN	15
Enrolls	Information to apply for new accounts	45
Skimmed	Duplicated magnetic track data from POS (Restaurant, Hotel, Retail, etc.)	40
Credit w/ PIN	Credit Card information plus PIN	175
Track2 w/ CVV2	Track 2 data plus the security code imprinted on the signature panel card	2
Visa / MC CC# w/CVV2	Transaction information plus security code	3
Balance Checking	Service provided by vendor to check available balance on stolen accounts	2
Phishing Pages	Scam pages of legitimate websites	100
Bank Logins	Compromised bank login username and passwords to bank cardholders	100

Pump & Dump

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

- SPAM Campaign
- Increasing in scale and sophistication
- Occurs in under one week
- Brokerage account(s) (stolen)
- Email sent (graphic) with nonsensical text “Bayesian poisoning”
- People buy, stock rises, scammer sells
- Example $.88, $1.28, $.13



Cyber Threats are Social

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

Facebook Statistics

paul C dwyer + ASSOCIATES
GRC & Cyber Threat Advisors

People on Facebook	More than 500 million active users 50% of our active users log on to Facebook in any given day Average user has 130 friends People spend over 700 billion minutes per month on Facebook
Activity on Facebook	There are over 900 million objects that people interact with (pages, groups, events and community pages) Average user is connected to 80 community pages, groups and events Average user creates 90 pieces of content each month More than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month.
Global Reach	More than 70 translations available on the site About 70% of Facebook users are outside the United States Over 300,000 users helped translate the site through the translations application
Platform	Entrepreneurs and developers from more than 190 countries build with Facebook Platform People on Facebook install 20 million applications every day Every month, more than 250 million people engage with Facebook on external websites Since social plugins launched in April 2010, an average of 10,000 new websites integrate with Facebook every day More than 2.5 million websites have integrated with Facebook, including over 80 of comScore's U.S. Top 100 websites and over half of comScore's Global Top 100 websites
Mobile	There are more than 200 million active users currently accessing Facebook through their mobile devices. People that use Facebook on their mobile devices are twice as active on Facebook than non-mobile users. There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products

500 Million Users

900 Million Objects

70 Languages

Installation of 20 Million Applications a Day

20 Million Mobile Users

Bottom Line

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

“……. Criminals go where people go…….”

10% of internet time is spent on social networking sites

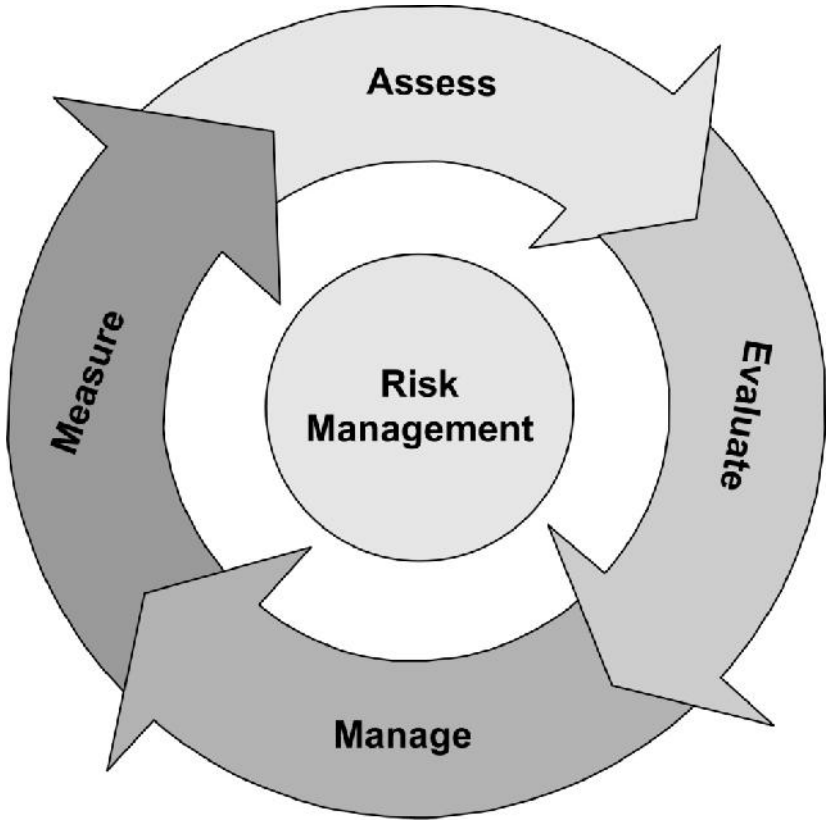
Facebook is the 3rd biggest ***country*** in the world!

CRO's and Cyber Threats

paul C dwyer + ASSOCIATES
SECURITY GRC & CYBER THREAT ADVISORS

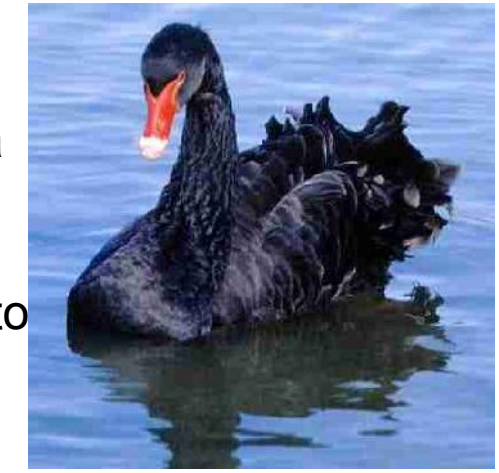
Automation: Cybercriminals can automate mundane tasks - making denial of service attacks and large scale junk mail possible, just as they enable 100% surveillance of the Internet communications traffic of any organisation.

Data collection: digital data requires minimal storage space and is easier to harvest and manipulate



CRO's and Cyber Threats

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors



Action at a distance: in cyberspace, the criminal who is targeting your network may be based in Chechnya, Moldavia or on a Pacific island.

Propagation: the Web enables ideas, skills and digital tools to be shared around the world within hours. It also enables techniques to be widely replicated and a vast array of computers to be linked into any one attack.

These main characteristics mean that when the bad guys finds a weakness, they can exponentially exploit it within seconds from multiple jurisdictions. This is completely different from the "normal" type of risk that generally a CRO considers.

Different Levels of Threat

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Low Hanging Fruit

Cyber Espionage

Targeted

Combination & “Low and Slow”

Major Players including Organised Crime

How Easy is All This?

How Easy is it to DDoS Someone?

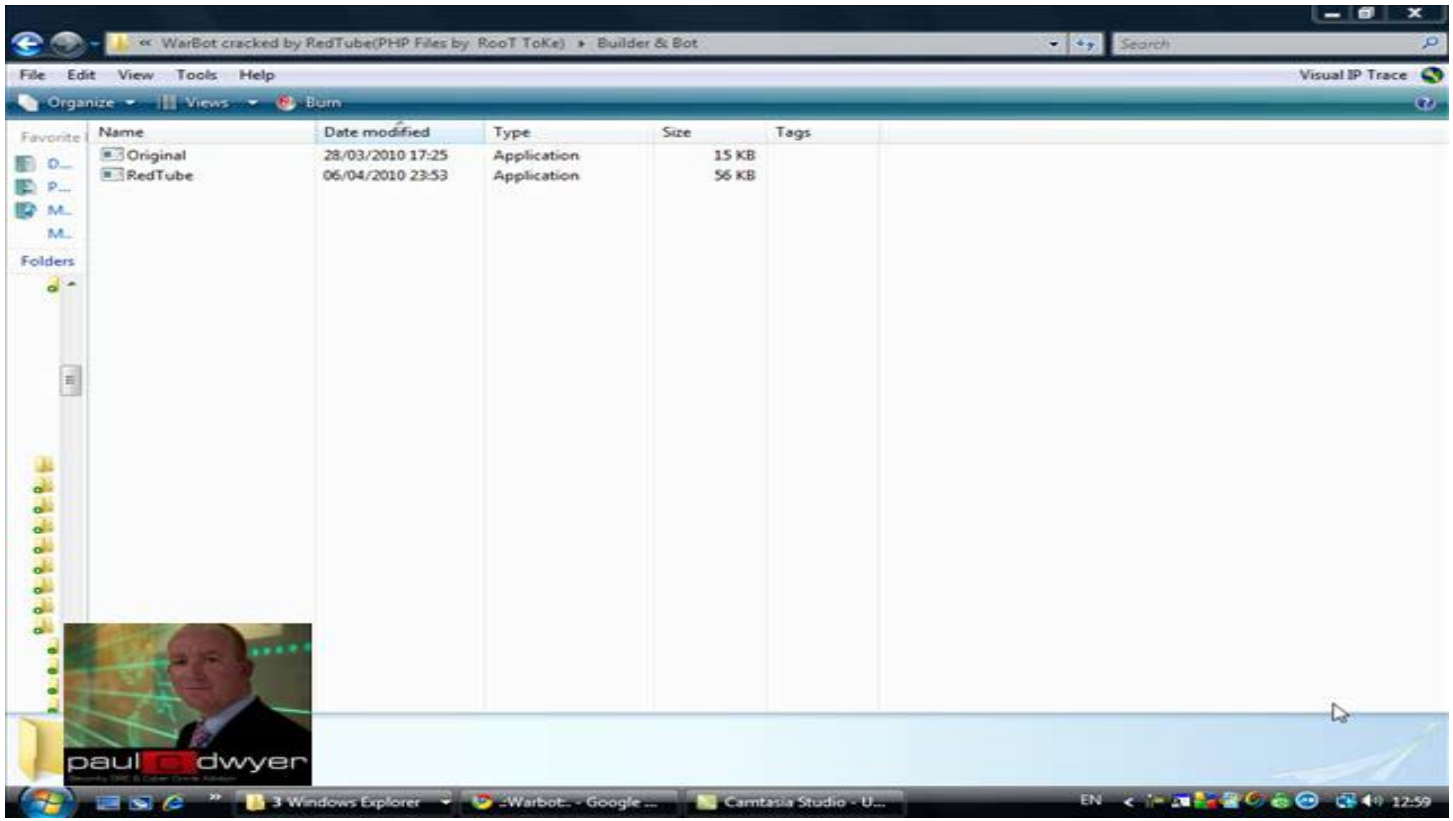
As Easy As…

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

1) Search on Google and Youtube
2) Download Toolkit
3) Follow Instructions
   a) Create Virus
   b) Attack Site

How Easy is a DDoS Attack

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors



Google
www.google.ie
Web Images Maps News Books Translate Mail more
paul@teaminfosec.com | iGoogle | Settings | Sign out
Google
Ireland
Advanced search
Language tools
Google Search
I'm Feeling Lucky
Google.ie offered in: Gaeilge
Advertising Programs
Business Solutions
About Google
Go to Google.com
© 2010 - Privacy
Change background image
paul dwyer
paul
Builder & Bot
Google - Google C...
Camtasia Studio - U...
EN
13:19

What's the Answer?

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Attribution?

Some Food for Thought

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

Defence? More boxes, The Castle

Proactive Cyber Defence means acting in anticipation to oppose an attack against computers and networks. It represents the dynamic between purely offensive and defensive action.

In the Fifth century, B.C., Sun Tzu (Art of War) advocated "foreknowledge" or predictive analysis as part of a winning strategy. He warned that planners must have a precise understanding of the active threat and not "remain ignorant of the enemy's condition.".

Collaborate with "competitors"

Disruption? e.g. Phishing poisoning

Offensive? e.g. DDoS

Thank you

paul C dwyer + ASSOCIATES
Security GRC & Cyber Threat Advisors

IRISH CYBER CRIME TASK FORCE

NACSRO

Blog LinkedIn Twitter YouTube

www.paulcdwyer.com