Security Matters : 26 May 2016
The Invisible Enemy

Michael Harris
Group Head of IT
Tokio Marine Kiln

Actors & Targets - 2015

Source: controlrisks.com
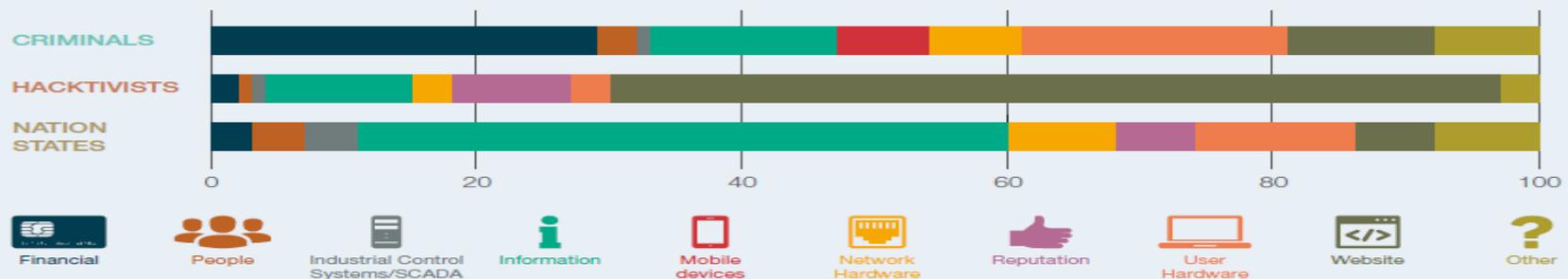
Why and how do they do it?
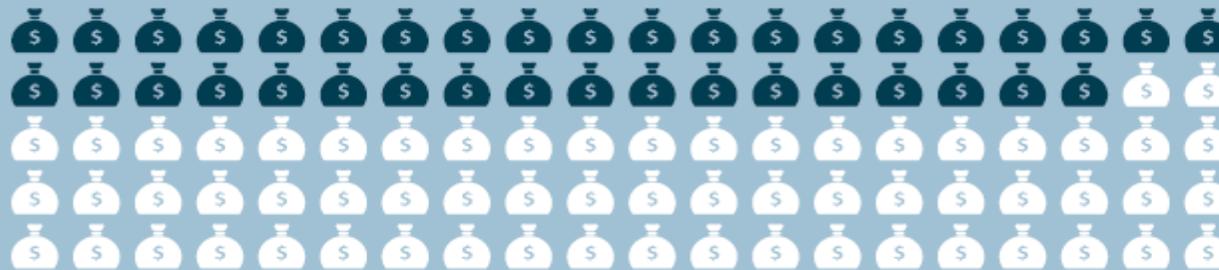
38% OF ATTACKS IN THE LAST 12 MONTHS WERE DRIVEN BY FINANCIAL GAIN

TOP 5 MOST WIDELY USED PRIMARY ATTACK METHODS IN THE LAST 12 MONTHS

01	02	03	04	05
Distributed Denial of Service (DDoS) attack	Single Purpose Malware	Advanced Persistent Threat Campaign**	Website defacement	Ransomware
M	H	H	M	H
5.6	7.0	7.6	5.1	7.7

CONTROL RISKS' THREAT SCORE* OF THE TOP ATTACK METHODS

*Control Risks' threat score considers the threat actors involved, the tools they use, the severity, impact and likelihood of success of the attack method. M=medium, H=high
**Use of a number of methods as part of an advanced multi-objective attack.

Source: controlrisks.com

Can you ignore it – regulation & reputation?

A combination of high-profile breaches, increased state and federal statutes and guidance and continued efforts to educate brokers and potential insureds may drive premium revenue to $2.75 billion by the end of 2015 and perhaps $7.5 billion by 2020, they predict. Tracy Dolin, Standard & Poor's Ratings Services analyst, estimated the market could reach $10 billion by 2025.

Source: Bloomberg

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Cyber Essentials
"Dear CEO" – August 2015

LLOYD'S

OP 1.1

IT Security and Infrastructure

Managing agents shall have appropriate IT systems and resilience for the management of the agency.

Managing agents shall:
- have appropriate IT infrastructure to manage the business;
- have appropriate technology to meet the business process and link with counterparty systems;
- have appropriate IT techniques in place to reduce the risk of cyber-attack;
- have appropriate controls to ensure data meets the requirements of the Data Protection Act 1998;
- be able to use the data held on their systems to populate both Lloyd's and PRA required returns; and
- give appropriate consideration to the necessary hardware and software to ensure the IT structure remains appropriate for the business.

NAIC
National Association of Insurance Commissioners

"Principles for Effective Cyber Security"

Facts & Figures – What's Happening?

"Cybercrime is big business—a trillion dollars a year"
University of West Florida

"A UK Government survey estimated that in 2014 81% of large corporations and 60% of small businesses suffered a cyber breach. The average cost of a cyber-security breach is £600k-£1.15m for large businesses and £65k-115k for SMEs"
Lloyd's of London

"We estimate that the likely annual cost to the global economy from cybercrime is more than $400 Billion"
McAfee

"40 percent of large enterprises will have formal plans to address aggressive cybersecurity business disruption attacks by 2018"
Gartner

"In the modern world it is a matter of *when*, rather than *if*, your organisation will be forced to deal with a cyber attack. 70 per cent of firms have suffered a "significant" breach in the last year"
Business Reporter

What can you do about it?

It's all about **people** and **communication** supported by **common sense** and **good practice**
Michael Harris

The Big Six Risks:

1) Disgruntled employees

2) Careless or uninformed employees

3) Mobile devices (BYOD)

4) Cloud applications

5) Unpatched or unpatchable devices

6) Third party service providers
Source: www.cio.co.uk