CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

CIMA

WHAT YOU ARE UP AGAINST COMBATING FRAUD

Garry W.G. Clement, CFE,CAMS, AMLP
President and CEO
Clement Advisory Group
905-355-1066, fax:905-355-3210
cell:905-375-5076
gclement@clementadvisorygroup.ca
www.clementadvisorygroup.ca

We are what we repeatedly do. Excellence, then, is not an act, but a habit.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

“Organized crime is so pervasive it demands coordination among federal government departments and intelligence agencies, the provinces, law enforcement agencies and private sector organizations. No single organization has responsibility for addressing this problem. We all must share information and work together to ensure Canada’s economic integrity.”
Canadian Bankers Association, Director of Security, William J. Crate

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

"It's snappy, it's today -- I like it."

Organized Crime

OC conceals criminal activity as a standard business practice. Use of fraudulently obtained or fictitious identities to register cell phones, to register companies, to purchase property, to lease vehicles, to conceal criminal records or to travel across borders is well documented.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

"As in other criminal fields, also in money laundering, organized crime groups display peerless skill in managing the international dimension, while national and international authorities are constantly struggling with it."

Europol 2008 Organized Crime Threat Assessment

EUROPOL

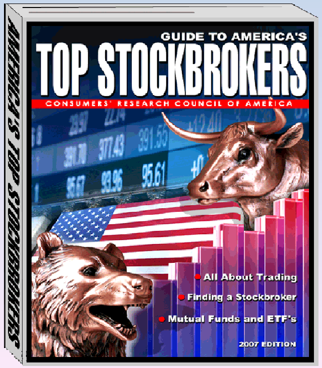
Corruption

To obtain access to information or thwart enforcement or regulatory processes, organized crime groups target a wide range of occupations to facilitate criminal activity. For example, the corruption or collusion of individuals working at points of entry continues to play a role in the international movement of illicit commodities. Targets of corruption and collusion can extend to a range of criminally inclined individuals being exploited from baggage handlers and ground crews, to various resource and supply services, as well as to law enforcement and public officials.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Organized crime groups target professional facilitators, such as lawyers, stock brokers, and accountants, to perpetrate securities fraud. They will often use virtual tools, such as e-mail and Internet sites like Facebook and YouTube, to efficiently and anonymously target victims worldwide and issue fictitious promotional material advertising fraudulent investment opportunities.



WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

2009 CISC REPORT

According to the Canadian Anti-Fraud Call Centre (CAFCC), Canadian based mass marketing fraud operations gross over $500 million per year. In 2008, Canadian victims of fraudulent mass marketing operations based in Canada reported losses of $26.9 million to the CAFCC, an increase of over $2 million from 2007. It is estimated only 5% of actual complaints are reported. The top reported mass marketing schemes last year included: service, prize (e.g. sweepstakes/lottery and gift), purchase of merchandise, sale of merchandise, job, vacation, collection agency and charity.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

CANADIAN
BANKERS
ASSOCIATION

Credit card fraud and Interac statistics provided by the Canadian Bankers Association shows combined annual losses due to debit and credit card fraud in Canada exceeded $500 million in 2008. Recorded losses from debit card fraud in Canada decreased slightly from losses in the previous year, while those from credit card fraud increased. The bulk of credit card fraud losses are attributed to counterfeiting and fraudulent purchases, suggesting an increase in organized criminal operations.

Money launderers going high-tech

Mobile phones, prepaid cards, online games. In the cat-and-mouse game of smuggling illicit money over international borders, criminal organizations are early adopters of new technology.

In particular, criminal gangs are increasingly using stored-valued cards to move cash.

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

“Deborah Morrisey, a supervisory special agent with the U.S. Department of Homeland Security, recently busted the money-laundering arm of a Colombian drug cartel that had operations in Miami. Over the course of nine months the group moved more than $4 million using stored-value cards, she said. The ring operated undetected until it was discovered by an undercover investigator. “

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Currently, hackers are targeting online sites and using malware and keystroke-logger programs to steal credit card data in order to bypass the need for skimming activity. This trend is likely to increase as online banking continues to grow in popularity. A transition from magnetic stripe debit and credit cards to ones embedded with microchip technology is currently underway in Canada; however, a complete implementation of the technology is expected to take several years. Furthermore, chip technology has no impact on the security of credit cards when used to purchase items online, by mail order or by phone

Hi-tech crimes including scams, hacking, identity fraud, and credit card skimming, are investigated by the Fraud and Corporate Crime Group

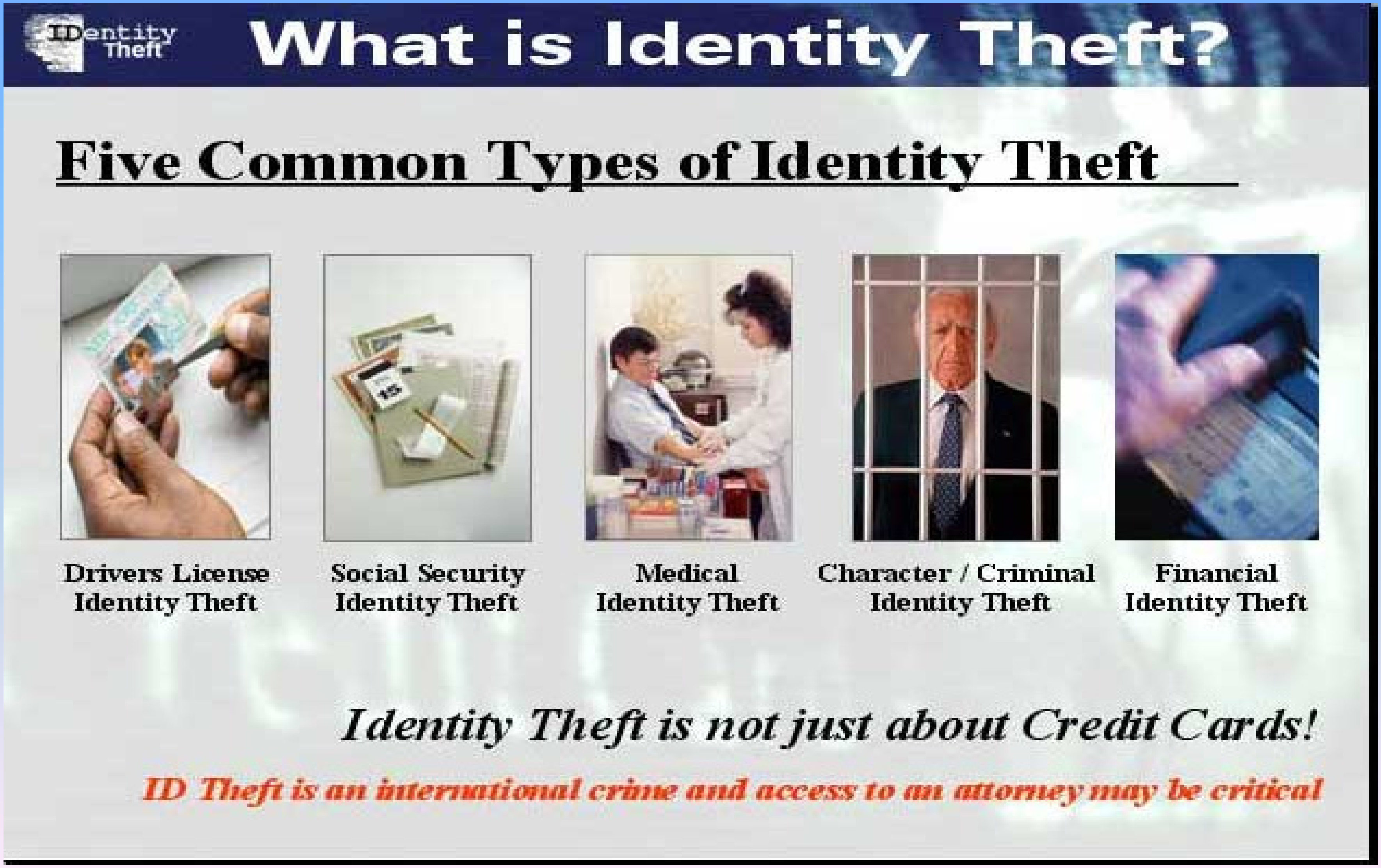
CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

IDENTITY THEFT

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION



IDentity Theft

What is Identity Theft?

Five Common Types of Identity Theft

Drivers License Identity Theft

Social Security Identity Theft

Medical Identity Theft

Character / Criminal Identity Theft

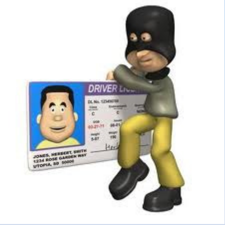
Financial Identity Theft

Identity Theft is not just about Credit Cards!

ID Theft is an international crime and access to an attorney may be critical

The Consequence of Identity Theft

- Identity thief seldom pays bills for debts incurred under victim name.
- Due to bad credit report, victim may be denied new credit, loans, mortgages, utility service, or employment.



- Where identity thief established criminal record in victim name, victim may fail background checks for employment, firearms, etc., or may even end up in jail.

Identity Theft

Identity Theft Is Often An Essential Component of Many Criminal Activities, From Bank and Credit Card Fraud to International Terrorism.

- An Algerian national facing federal charges of identity theft allegedly stole the identities of 21 members of a health club transferring them to one of three Algerians convicted in a failed 1999 plan to bomb Los Angeles International Airport.

Identity Theft

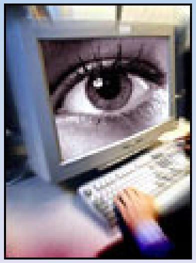
Identity Theft is the Fastest Growing Crime in the United States and Canada

- The Privacy Rights Clearinghouse estimates that between 500,000 and 700,000 people each year become victims of identity theft.
- Losses to credit card fraud, the most popular form of identity theft, totaled an estimated $1.6 billion in 2008.
- In almost 1300 complaints received by the FTC, identity theft victims said they have been subjected to “criminal investigation, arrest, or conviction.”

How Identity Theft Occurs

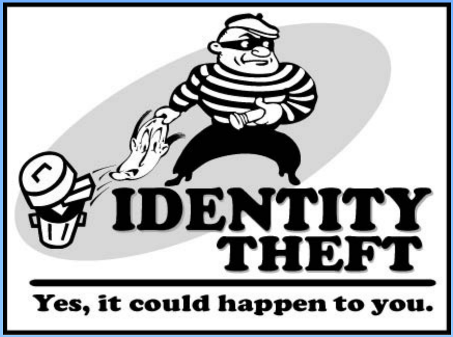
Identity thieves…

- steal wallets and purses containing your ID
- steal your mail
- complete false “change of address” forms
- rummage through trash (“dumpster diving”)
- pose fraudulently as someone else to get your information



CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION



Examples of methods used to acquire personal information:	Examples of fraud committed using personal information without authorization:
Corrupt employees Fraudulent mass marketing Theft (mail, wallet) Break and Enters into residences, vehicles and businesses Dumpster diving*2 Phishing*, Pharming*, Spyware* Unauthorized access to computer Mischief to data Internet open sources Social engineering*	Payment card fraud Cheque fraud Mortgage/title fraud Insurance fraud Government program/service/benefit fraud Government document fraud Immigration fraud Bank fraud (fraudulent accounts, account takeovers, loans) Account fraud (cell phones) Election fraud

Mortgage Fraud - rising

Equifax uncovered $400 million worth of mortgage fraud last year an estimated fraction of reality of roughly $1 trillion in total residential mortgage credit outstanding in Canada.

How:

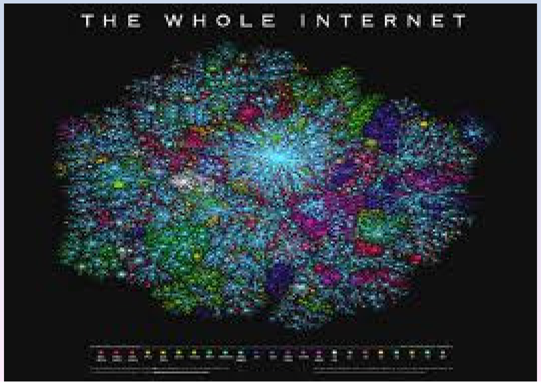
- O.C.: using industry insiders such as property agents, mortgage brokers and lawyers
- Establishment of fictitious identities, building credit in fake names and then borrowing: Equifax last year identified over 2500 fake names

Cyber Crime

At $388bn, cybercrime is more than **100 times the annual expenditure of UNICEF** ($3.65 billion)

INTERNET REALITY

➢Users in Developing Countries	1.2 billion
➢Developed Country	850 million
➢Access to Mobile Phones: Developing	7 out of 10
➢China accounts 40% of Internet access	
➢Text messages sent annually worldwide	6.1 trillion



Cyber Crime Current Realities:

- It could shut down our electric grid or water supply. It could cause serious damage to parts of our cities, and ultimately even kill people
- Intrusions into corporate networks, personal computers, and government systems are occurring every single day by the thousands

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Cyber Crime Actors:

- Foreign intelligence services, terrorist groups, and organized crime enterprises
- (Dozens of countries have offensive cyber capabilities, and their foreign intelligence services are generally the most capable of cyber adversaries.)

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

A defector from China’s intelligence services has indicated China has 1,000 economic spies at work in Canada, more than any other country. Canadian researchers have been instrumental in uncovering a worldwide software-based Chinese spy network that targeted sensitive government information, while industrial espionage has pillaged Canadian industrial and business secrets.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Nortel collapse linked to Chinese hackers

Corporate espionage continues against Canadian firms, security expert says

A former systems security adviser to Nortel Networks says he has no doubt that extensive cyberattacks on the technology company contributed to its downfall.

Case Examples:

- An international network of hackers obtained access to a financial corporation’s network and completely compromised its encryption. They were inside the system for months doing reconnaissance, which enabled them to steal millions of dollars in less than 24 hours when they finally took overt action.

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Major international hacking group used an Automated Clearing House (ACH) wire transfer system to access online commercial banking accounts and distribute malicious software that led financial institutions to lose nearly $70 million.

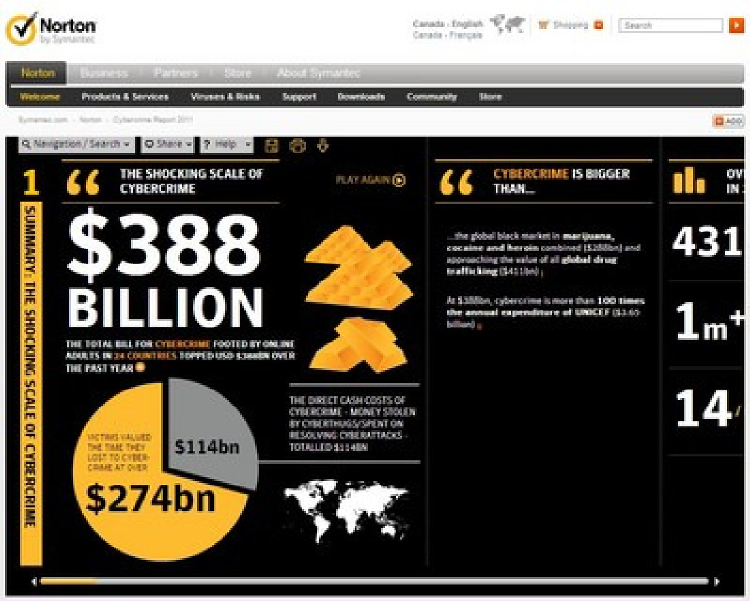
A U.S. company that was recently the victim of an intrusion determined it had lost 10 years worth of research and development—valued at $1 billion—virtually overnight.

Members of the Brazilian team at Farmanguinhos.

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

The 2011 Norton Cybercrime Report put the global cost of cyber crime at nearly $400 billion a year, and found that there are more than one million victims of cyber crime every day.



THE SHOCKING SCALE OF CYBERCRIME

$388 BILLION

THE TOTAL BILL FOR CYBERCRIME FOOTED BY ONLINE ADULTS IN 24 COUNTRIES TOPPED USD $388BN OVER THE PAST YEAR

VICTIMS VALUED THE TIME THEY LOST TO CYBER-CRIME AT OVER $274bn

$114bn

THE DIRECT CASH COSTS OF CYBERCRIME - MONEY STOLEN BY CYBERTHUGS/SPENT ON RESOLVING CYBERATTACKS - TOTALLED $114BN

CYBERCRIME IS BIGGER THAN...

...the global black market in **marijuana, cocaine and heroin** combined ($288bn) and approaching the value of all **global drug trafficking** ($411bn)

At $388bn, cybercrime is more than **100 times the annual expenditure of UNICEF** ($3.65 billion)

- Two thirds of online adults (69 percent) have been a victim of cybercrime

CLEMENT ADVISORY GROUP

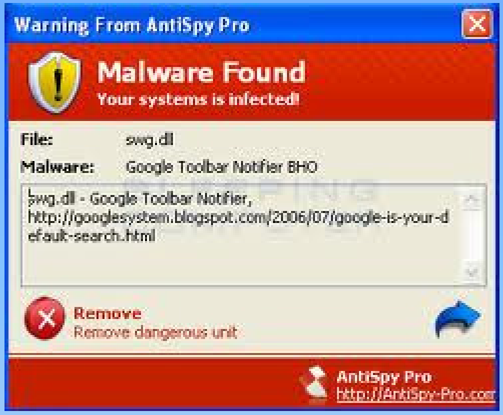
WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

10% of all adults surveyed have experienced cybercrime on their mobile device .

A study released in August by the Ponemon Institute found that the number of attacks on companies it surveyed this year were up 45 percent from last year and cost 70 percent more to fix. On average, each attack took 18 days and $416,000 to fix.

Risk equals threat times vulnerability times consequence.'

If we lower any of those three variable factors, we lower the risk. If we can completely eliminate any of those variables, we eliminate risk. But that's virtually impossible, so we must adopt a defense-in-depth approach—lowering each of the three.



Warning From AntiSpy Pro

Malware Found
Your systems is infected!

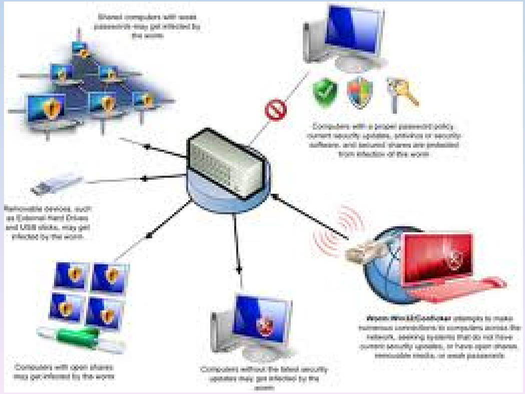
File: swg.dll
Malware: Google Toolbar Notifier BHO

swg.dll - Google Toolbar Notifier,
http://googlesystem.blogspot.com/2006/07/google-is-your-default-search.html

Much of the newest malware is being deployed through social engineering schemes or through third-party applications on social networking sites, like Facebook (but by no means limited to them), often in the form of suggested plug-ins, games, and new friend requests.

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

Under the current environment, victims are often focused on how to get malware off their systems and on finding out what was taken. But what they should be asking is, ‘What was left behind? And did it change my data?’ Most users have no idea whether their software, hardware, or data integrity has been altered. Our current networks were never designed to detect that type of deviation.


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of the worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm.
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

What needs to be secured.

On the technical side:

The web servers, e-mail servers, databases, firewalls, routers, embedded network devices, internal networks, remote access, custom applications, off-the-shelf applications, backup and storage areas, and all telephone, PBX, and VoIP systems.

On the human side,
Secure your physical infrastructure, employee accesses and permissions, and connections to business and corporate partners. These are just the basics on the way to a secure network, all of which need to be monitored and updated regularly, as the technologies change constantly and so do our users.

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

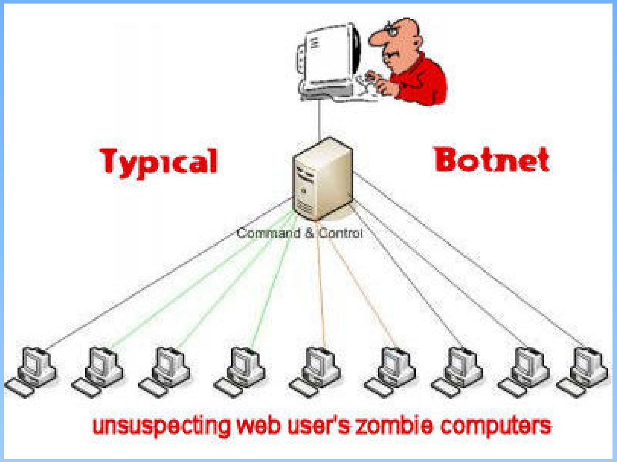
10 specializations we see in a typical cyber crime.

1. The coders or programmers, who write the malware, exploits, and other tools necessary to commit the crime.
2. The distributors or vendors, who trade and sell stolen data, and act as vouchers of the goods provided by the other specialties.
3. The techies, who maintain the criminal infrastructure, including servers, bulletproof ISPs, and encryption; and who often have knowledge of common database languages and SQL servers of course.

4. The hackers, who search for and exploit application, system, and network vulnerabilities to gain administrator or payroll access.
5. The fraudsters, who create and deploy social engineering schemes, including phishing, spamming, and domain squatting.
   work, the next is tried.

6. The hosters, who provide “safe” hosting of illicit content servers and sites, often through elaborate botnet and proxy networks.
7. The cashers, who control drop accounts and provide those names and accounts to other criminals for a fee, and who also typically control full rings.
8. The money mules.

9. The tellers, who help with transferring and laundering illicit proceeds through digital currency services and between different world currencies.
10. The leaders—many of whom don’t have any technical skills at all. They’re the “people-people.” They choose the targets; choose the people they want to work each role; decide who does what, when, and where; and take care of personnel and payment issues.

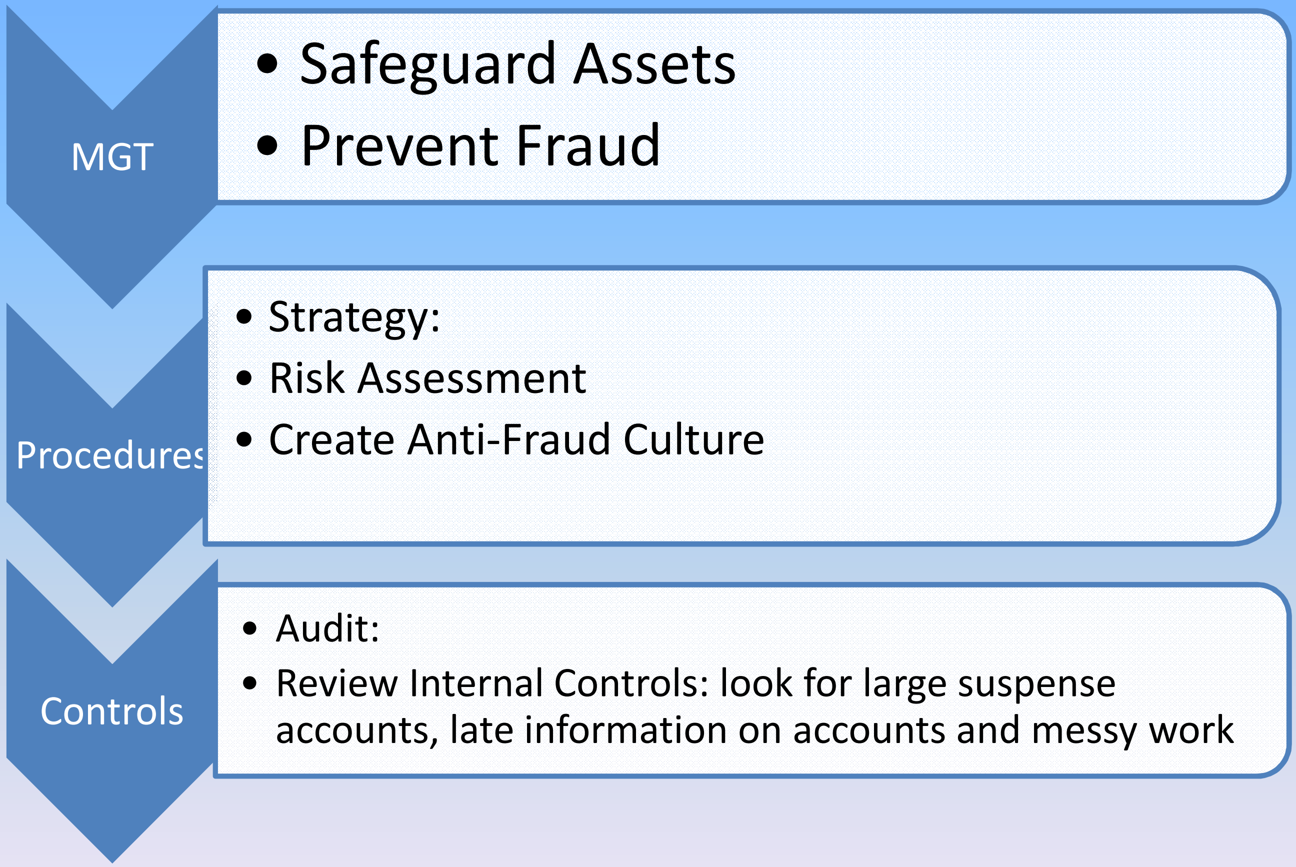


A number of botnets, like Haxtor, are specifically leased out to criminals for proxying their malicious activities. Rather than typical random proxying services, criminals can choose which nodes of the botnet they would like to use based on up-time, connection speed, and other factors.

There are 3 general strategies for preventing, detecting, and deterring fraud.

1. Passive – Reliance is placed on internal controls to prevent, detect and deter fraud
2. Reactive – Reliance is placed on investigation after fraud occurs
3. Proactive – Reliance is placed on tools and methods to routinely search for fraud indicators

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION



MGT

- Safeguard Assets
- Prevent Fraud

Procedures

- Strategy:
- Risk Assessment
- Create Anti-Fraud Culture

Controls

- Audit:
- Review Internal Controls: look for large suspense accounts, late information on accounts and messy work

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

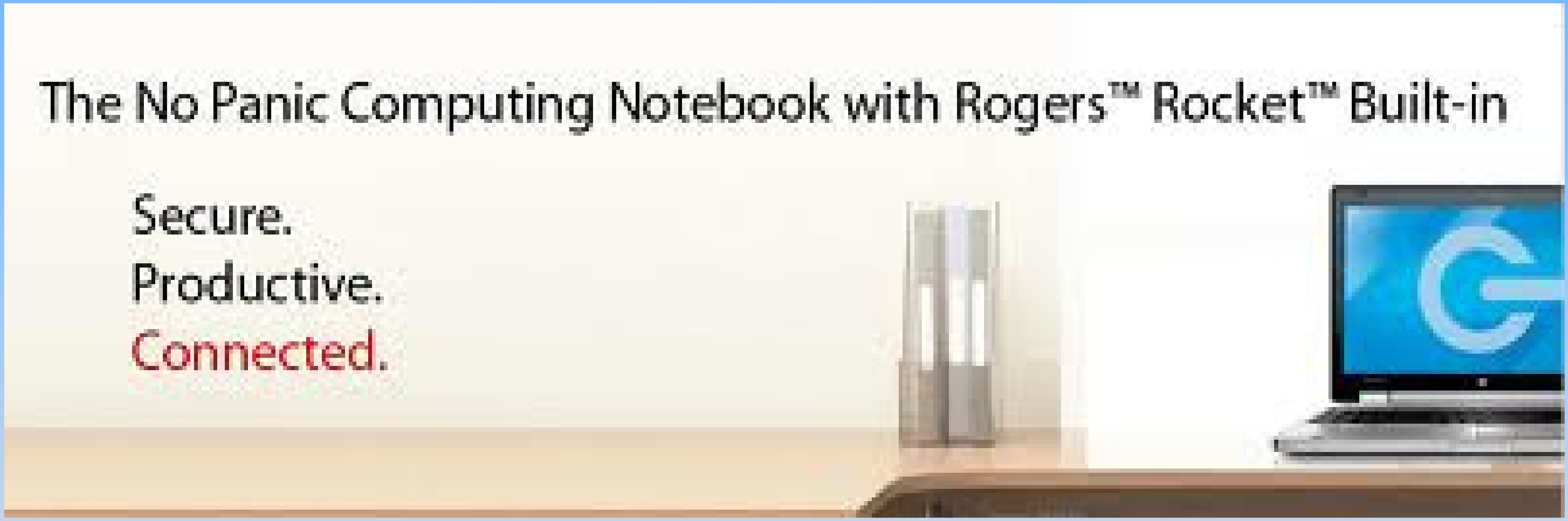
TOP 5 STRATEGIES FOR FRAUD PREVENTION AND DETECTION

LARGE CAP	MID CAP	SMALL CAP	PRIVATE	NOT-FOR-PROFIT
BUSINESS ETHICS PROGRAM	BUSINESS ETHICS PROGRAM	INTEGRATE FRAUD AUDIT PROCEDURES AND TESTING OF INTERNAL CONTROLS	BUSINESS ETHICS PROGRAM	INTEGRATE FRAUD AUDIT PROCEDURES INTO TESTING OF INTERNAL CONTROLS
INTEGRATE FRAUD AUDIT PROCEDURES INTO TESTING OF INTERNAL CONTROLS	DATA MINING TOOLS AND/OR TECHNIQUES	BUSINESS ETHIC PROGRAMS	MONITORING KEY FRAUD INDICATORS	BUSINESS ETHICS PROGRAM
MONITORING KEY FRAUD INDICATORS	INTEGRATE FRAUD AUDIT PROCEDURES INTO TESTING OF INTERNAL CONTROLS	MONITORING KEY FRAUD INDICATORS	CONTINUOUS AUDITING TOOLS AND/OR TECHNIQUES	MONITORING KEY FRAUD INDICATORS
FRAUD AWARENESS: COMMUNICATING FRAUD SCHEMES AND RED FLAGS	INTEGRATE FRAUD AUDIT PROCEDURES INTO TESTING OF INTERNAL CONTROLS	FRAUD TRAINING	INTEGRATE FRAUD AUDIT PROCEDURES INTO TESTING OF INTERNAL CONTROLS	FRAUD AWARENESS: COMMUNICATING FRAUD SCHEMES AND RED FLAGS
FRAUD AUDIT PROGRAM	FRAUD AWARENESS: COMMUNICATING FRAUD SCHEMES AND RED FLAGS, MONITORING KEY FRAUD INDICATORS, FRAUD TRAINING, FRAUD RESPONSE POLICY	FRAUD RESPONSE POLICY	FRAUD AWARENESS: COMMUNICATING FRAUD SCHEMES AND RED FLAGS	CONTINU0US AUDIT TOOLS AND/OR TECHNIQUES FRAUD TRAINING FRAUD AUDIT PROGRAMS

VONYA GLOBAL SURVERY

CLEMENT ADVISORY GROUP

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION


The No Panic Computing Notebook with Rogers™ Rocket™ Built-in
Secure.
Productive.
Connected.

WHITE COLLAR INVESTIGATIONS | ANTI-MONEY LAUNDERING
COMPLIANCE | RISK MITIGATION

THANK YOU

Clement Advisory Group is a premier consulting and investigative firm that focuses on the financial and governmental sectors. We are comprised of professionals that strive to achieve results that exceed expectations through Our Commitment to Our Clients, adding maximum value to their programs and/or business through:

- ***Handling complex and sophisticated matters locally, nationally and internationally***
- ***Being accessible, efficient, responsive and technologically sophisticated***
- ***Being committed to our communities***
- ***Promoting active involvement and leadership on the part of our firm and ourselves***
- ***Sustaining an enriching environment through diversity and teamwork***
- ***Assuring opportunities by sustaining growth and financial strength***