CRI|GROUP
Corporate Research and Investigations

RESEARCH STUDY

RISKS OF CYBERCRIME & SOCIAL MEDIA

COMPLETE GUIDE ON HOW TO PROTECT YOUR ORGANISATION AND TEAM!

Take the first steps towards developing measures against cybercrime! This paper critically examines the growth of cybercrime, evaluating the risks it poses in terms of the different forms of cybercrime that exist and the regulations that seek to detect, prevent and punish them.

ABSTRACT

The PwC Global Economic Crime Survey 2020 found that a company falls victim to six frauds on average. The most common types were customer fraud, asset misappropriation and cybercrime. And there was a roughly even split between frauds committed by internal and external perpetrators, at almost 40% each – with the rest being mostly collusion between the two.

Few can deny the enormous technological advancements that are constantly taking place in the modern world. The internet, the computer, and other technological advancements have dramatically changed what it means to socialise, 'chat', and even read a book. Both the disadvantages and advantages of such developments are clear, and as technology gains pace, so have the unlawful activities of those who seek to take advantages of such developments.[1]

According to a 2020 cybercrime report from Europol, COVID-19 sparked upward trend in cybercrime. In fact, since the beginning of the pandemic, the FBI has seen a fourfold increase in cybersecurity complaints, whereas the global losses from cybercrime exceeded $1 trillion in 2020. As the technology evolves, cybercrimes have become complex and the sense that one is safe from crime in the privacy of one's own home has been lost. In fact, according to World Economic Forum's "Global Risks Report 2020" the chances of catching and prosecuting a cybercriminal are almost nil (0.05%).

This playbook will critically examine the growth of cybercrime, evaluating the risks it poses in terms of the different forms of cybercrime that exist and the regulations that seek to detect, prevent and punish them. Such analysis will be shown to reveal that the extension of old legislation to include cybercrime is not entirely effective,[2] particularly concerning crimes committed within the realm of social media and social networking.[3] Thus emerges the need to develop an 'anti-cybercrime culture on an international scale so that safeguards and the promotion of careful use can be facilitated to hinder such crimes before they can materialise.

Keywords: 'cybersecurity' and 'anti-cybercrime'

WHAT IS CYBERCRIME & WHY IS IT IMPORTANT?

The PwC Global Economic Crime Survey 2020 found that a company falls victim to six frauds on average. The most common types were customer fraud, asset misappropriation and cybercrime. And there was a roughly even split between frauds committed by internal and external perpetrators, at almost 40% each – with the rest being mostly collusion between the two.

Cybercrime is commonly defined as the commission of a crime against or through the use of technological mechanisms such as the internet, software and computer data.4 While cybercrime is a relatively new form of crime, it ultimately can be defined as a method by which traditional crimes are committed.

Chik & Bartholomew state that "What we call cybercrime largely consists of common crime, the commission of which involves the use of computer technology, and for which penalties already exist under existing legislation".[5]

In this respect, it could be stated that cybercrime relates to a new medium through which more traditional crimes such as fraud may be committed.[6] However, new forms of crime such as hacking have emerged as a result of such technology.[7] This, of course, does not mean that cybercrime may be approached in the same manner as such traditional crimes. Indeed, the threat of such crimes when committed through technological mediums is considerably more significant because it provides the offender anonymity, privacy, and expansive access to his victims.[8]

According to the Internet Organised Crime Threat Assessment (IOCTA), cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including high-tech crimes, data breaches, laundering traditional and virtual currencies; the online hosting of operations involves selling weapons, false passports, counterfeit and cloned credit cards, and drugs; hacking services and sexual extortion. With cryptocurrencies continuing to facilitate payments for various forms of cybercrime.

The huge increase in the use of social media such as Facebook and Twitter has undoubtedly facilitated the development of new forms of criminal behaviour and the occurrence of more traditional criminal conduct.[9]

Facebook has, for example, arguably obliterated the levels of privacy that individuals can expect and maintain as one's social life has become potentially

available for all to observe and abuse. Online virtual gaming sites have seen, for example, the use of 'voodoo dolls'[10] to commit a form of identity theft and virtual rape.[11]

Despite the existence of fraud in traditional criminal law, its characteristics and forms when committed in the cybercrime sphere have provoked some to call for its definition as a new type of crime.[12]

Modern technology allows fraud (and most other types of crimes) to become anonymous, long-distance,[13] broad in scope and relatively effortless.[14] These characteristics serve to distinguish cyber-fraud from its traditional counterpart, suggesting that existing regulations may not be suitable for this type of cybercrime.

The careless manner in which social media is used provides almost limitless potential for offenders; in 2011, the Fawkes Virus released by Anonymous intercepted Facebook users' accounts and sent malicious messages to their contacts.[15]

Online theft provides another example of cybercrime, resulting in a greater loss than traditional theft. At the same time the average bank robbery in the U.S. amounts to less than $8,000 netted by offenders,[16] online bank theft allowed Vladimir Levin to net $12 million from the accounts of Citibank customers.[17] JPMorgan endured a huge cyber security breach in 2014, when hackers compromised the data of its banking customers.

The cybercriminals gained access to 76 million household accounts and seven million small business accounts. Such incidents demonstrate the huge scale of cybercrime and the irrelevance of national borders and geographical factors.

The risk of cybercrime is extremely prominent; its frequency and the losses that it causes are huge. According to PwC's Global Economic Crime and Fraud Survey 2020, the total cost of these crimes is an eye-popping US$42 billion. That's cash taken straight off companies' bottom line. And 13% of those who'd experienced a fraud said they'd lost US$50 million-plus.

For countries such as the EU Member States, the number and frequency of cybercrime cases are rising. As the internet infrastructure is well developed and payment systems are online, these countries are prime for attacks not just for their financial data but also for data generally. This, in turn, leads to more cases of fraud and extortion.

At CRI® we know that data security is a topic at the top of your business plan. Having a strong plan to protect your organisation from cyberattacks is key to your business continuity plan and will help you deal with the aftermath of a potential security breach. Talk to our team NOW!

GET A FREE QUOTE NOW!

ARE YOU MAKING INFORMED DECISIONS?

CRI® recommends background screening investigations as key proactive measures to help keep your business safe from the vendor and third-party screening to employment screening. An effective background screening will help screen for bad apples that can cause havoc down the road.

Background investigations are critical to any company's success because working with qualified, honest, hard-working employees and other businesses is an integral part of thriving in the business community. What you don't know can hurt you, and the simple act of one bad decision can result in an unprecedented loss for your company.

THE GLOBAL LEADER IN BACKGROUND SCREENING INVESTIGATIONS

Because we maintain a diverse talent base comprised of multilingual and multi-cultural professionals, CRI® can traverse obstacles that often impede international background screening investigations. That's why our competitors frequently contract us to conduct background screening in geographic regions not serviced or accessible by larger investigative firms. In fact, background screening firms worldwide use CRI® to conduct background screening in remote areas globally, where we can produce quality results that meet the constraints of tight timeframes and restricted budgets.

INVESTIGATIONS BROCHURE

We are always ready to assist you to effectively manage your workplace in an efficient and risk-free manner that best suits your needs. Our experience base, skilled workforce, technical resources, networking capabilities, internal flexibility and global offices maximise our solution efficacy. Explore our broad range of risk management solutions for your business.

CRI® Group's investigators and Certified Fraud Examiners understand the patterns of fraud and are trained to recognise the elements of fraud characteristics and where they might come into play at any organisation. It is through this knowledge that we can help you uncover the trail of fraud and help bring about a quick and successful resolution.

Having global coverage, CRI® works directly with the key personnel to lead and conduct fraud investigations, including, if needed, your internal board of directors, audit committee, ethics and compliance officers, general and in-house counsel, corporate security, human resources, and C-level executives.

RISK MANAGEMENT SOLUTIONS BROCHURE

DATA BREACH IS A SECURITY DISASTER

CRI Group's corporate due diligence services experts ask the hard questions, especially to any organisation conducting business on a global level. For example:

HOW DO YOU MANAGE THE RISKS TO DIGITAL AND PHYSICAL ASSETS?

CRI Group can put measures in place that provide layers of cybersecurity resilience to thwart hackers and those trying to steal your data.

HOW QUICKLY CAN WE RESPOND TO A SERIOUS BUSINESS CRISIS?

CRI Group's corporate due diligence services can help you detect breach attempts before they succeed and have a chance to damage your business.

CAN THE ORGANISATION RELY ON OUR THIRD-PARTY BUSINESS PARTNERS TO MAINTAIN APPROPRIATE LEVELS OF CONTROL?

One of your biggest risks is what happens outside of your organisation. Our third party risk management and due diligence services can help detect weaknesses among your partners and alert you to risk areas.

GET A FREE QUOTE NOW!

TOP CORPORATE CYBERSECURITY RISKS

SOCIAL ENGINEERING OR/AND UNINTENDED DATA LEAKS:

Social engineering remains a top threat to facilitate other types of cybercrime. Internet security companies continuously highlight the human factor as the weakest link in cyber security. This is evident, for example, when employees or managers unwittingly make huge amounts of data public – accidentally emailing an Excel file with personal data or placing it online. These unintended data leaks not only undermine the reputation of your company but can also lead to substantial fines. The new European General Data Protection Regulation (GDPR) significantly increased the authority of the Privacy Commission.

THE SOLUTION:

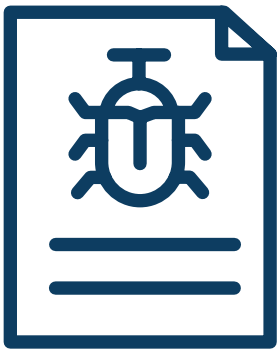
Increase awareness of the threat of unintended data leaks by educating your team on how to combat this type of cyber risk. Implement mandatory workshops and send warnings emails on how they can prevent data leaks.

VIRUS ATTACKS VIA PHISHING:

These large-scale attacks are carried out daily by malicious organisations. When you are a target of phishing, you or someone at your organisation receives an email containing a harmful file or a link to a harmful file. When you open the file or click the link, the virus is activated. Gerrit Mets, a cyber expert at Vanbreda Risk & Benefits, said “The consequences of phishing can be severe. The virus can bring down a company’s entire IT system, leak data, or block the system until it pays a ransom. In each of these cases, the organisation suffers reputational damage as well as substantial financial damage. For example, the ‘clean up’ of an IT system following a cyberattack can cost a tidy sum.”

THE SOLUTION:

Phishing gangs are becoming increasingly inventive. The emails are written in perfect English, and anti-virus software cannot always keep the most damaging viruses at bay. It is, therefore, crucial to making people at your company aware of this threat. Ensuring that emails and files are only opened after checking who sent the email is a step in the right direction. For more information, visit www.safeonweb.be.

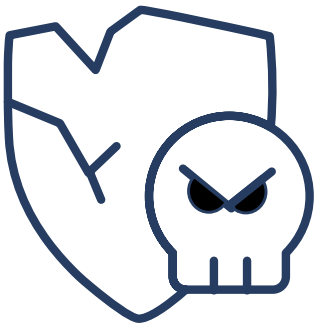


PUBLIC WEBSITE HACKS:

More often than not these are implemented by political groups that hack websites to spread propaganda and extract ransom money. However smaller companies are particularly susceptible since they often do not have the correct security technology and procedures to withstand this type of cyberattack. The reputational damage is often substantial with customers drawing on the rather logical conclusion, “if they can’t even secure their website, how can they keep my data safe?”

Equifax learned this the hard way after a 2017 data breach that compromised the personal data of 147 million customers. As a result of subsequent litigation, the company agreed to pay up to $425 million to assist affected individuals. The costs of this type of attack will add up, and more so if you use your website as a sales channel.

THE SOLUTION:
Ensure that you have the right software and procedures to secure your website by engaging the services of companies that offer the right expertise.



HACKING VIA OUTDATED SOFTWARE:

your company uses computer software that need updating regularly, you inevitably have a higher risk of falling victim to cybercrime. If you do not update your software in time, this creates ‘vulnerabilities’ in your system that hackers can ruthlessly exploit to break into your system.”

THE SOLUTION:
Ensure that your software is updated in time and always carry out updates as soon as the software requests it. This is certainly essential if you use systems and software that are connected to the internet. It’s just as important to keep your wireless router updated.

LET'S GET TECHNICAL: 10 TYPES OF HIGH-TECH CRIMES

High-tech crime is everything from a malware, or malicious software, that infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware:

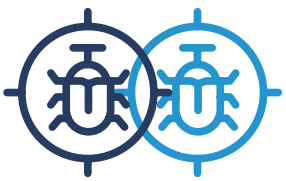
TROJAN poses as or is embedded within a legitimate programme. Still, it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks;

ADWARE displays advertising banners or pop-ups that include code to track the user's behaviour on the internet;

SPYWARE is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party;

SCAREWARE is fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed;

ROBOT NETWORK (A.K.A BOTNET): comprises computers creating "back doors" by communicating with each other over the internet. A command and control centre uses them to send spam, mount distributed denial-of-service (DDoS) attacks and commit other crimes such as the theft of money and data, or remote access to the devices to create more botnets;



WORM replicates itself over a computer network and performs malicious actions without guidance;

ROOTKIT is a collection of programmes that enable administrator-level access to a computer or computer network, allowing the attacker to gain root or privileged access to the computer and possibly other machines on the same network;

FILE INFECTOR infects executable files (such as .exe) by overwriting them or inserting infected code that disables them;

BACKDOOR/REMOTE-ACCESS TROJAN (RAT) accesses a computer system or mobile device remotely. Another piece of malware can install it. It gives almost total control to the attacker, who can perform a wide range of actions, including:

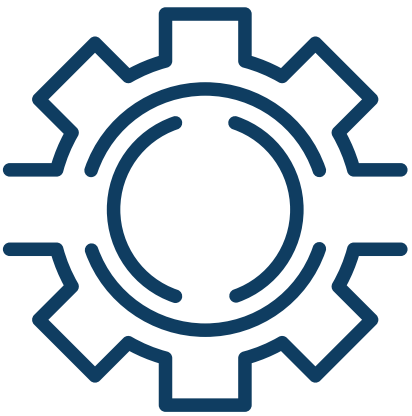
- monitoring actions
- executing commands
- sending files/documents back to the attacker
- logging keystrokes
- taking screenshots

RANSOMWARE remains the most dominant threat. Criminals can stop workers from accessing their IT systems and devices, and demand that they pay a ransom through certain online payment methods to regain access or simply threaten them with the publication of data if victims do not pay. According to Hiscox, 6% of companies paid a ransom in 2019, creating $381 million in losses.

→ **Human Capital can make (or break) your business - most organisations manage some of their risks via an insurance policy and risk retention. However, this is a reactive strategy when it comes to risk.**

If you are one of these organisations, then you are missing the riskiest part of the equation: people risk. Explore more on how to mitigate employee risk here!

HOW CYBERCRIME IMPACTS YOUR BUSINESS & YOUR COMPANY'S GROWTH



OPERATIONAL DISRUPTION:

Businesses face indirect costs from cyberattacks, such as major interruption to operations that result in lost revenue.

Cybercriminals can use any number of ways to handcuff a company's normal activities, whether by infecting computer systems with malware that erases high-value information, or installing malicious code on a server that blocks access to your website.

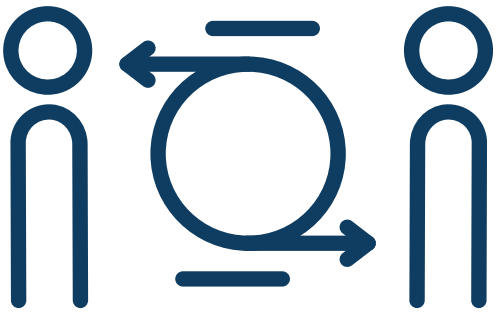
Disrupting business as usual is the favored tool of so-called "hacktivists," who have been known to breach the computer systems of government agencies or multinational corporations in the name of calling out a perceived wrong or increasing transparency. For example, in 2010 WikiLeaks 'supporters' retaliated against credit card giants Mastercard and Visa by conducting an 'operation payback' attack that temporarily crashed their websites.

INCREASED COSTS:

In order for businesses to protect themselves from cybercrime they have to invest in:

1. cybersecurity technology and expertise;
2. notifying affected parties of a breach;
3. insurance premiums; and
4. public relations support.

In addition, businesses may have to hire lawyers and other experts to remain compliant with cybersecurity regulations. And if they're the victim of an attack, they may have to shell out even more for attorney fees and damages as a result of civil cases against the company.



REPUTATIONAL DAMAGE:

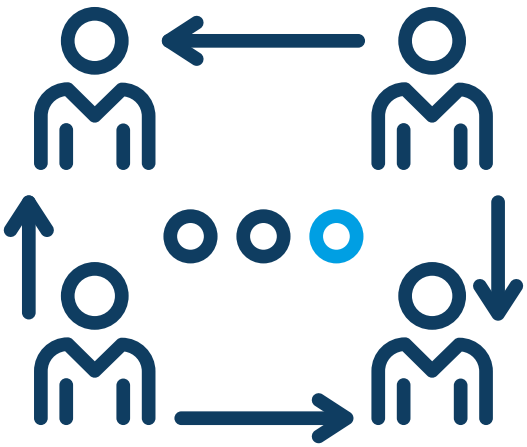
Organisations that fall victim to larger cyberattacks find their brand equity significantly tarnished. Customers, and even suppliers, are more likely to feel less secure leaving their sensitive data in the hands of a company whose IT infrastructure was broken at least once before.

In 2013 TGT saw its brand equity take a hit has they got involved in a huge data breach of more than 40 million customers credit card details, costing the company $18.5 million to settle. In addition to reduced institutional trust, research suggests that publicly traded companies are likely to see a short-term drop in market value.

According to the security researchers Comparitech, who studied 40 data breaches at 34 companies listed on the New York Stock Exchange (NYSE), the share prices of compromised companies fell an average of 3.5% following a cyberattack, and underperformed the Nasdaq by 3.5%.

→ **Our team of experts can help safeguard your business from unseen threats such as employee fraud, internal investigations, conflict of interest, compliance issues and other concerns that can quickly — and severely — impact any organisation in any part of the world.**

GET A FREE QUOTE NOW!

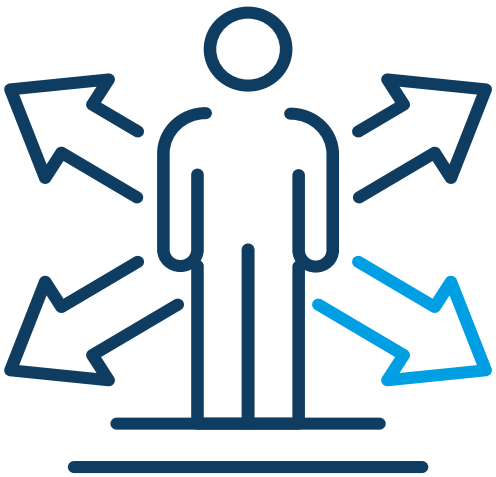


ALTERED BUSINESS PRACTICES:

Cybercrime can impact businesses in more than just financial ways. Companies have to rethink how they collect and store information to ensure that sensitive information isn't vulnerable.

Many companies have stopped storing customers' financial and personal information, such as credit card numbers, Social Security numbers, and birth dates. Some companies have shut down their online stores out of concern they cannot adequately protect against cyberattacks.

Customers are also more interested in knowing how the businesses they deal with handle security issues, and they are more likely to patronise businesses that are up front and vocal about the protections they have installed.



STOLEN INTELLECTUAL PROPERTY:

A company's product designs, technologies, and go-to-market strategies are often among its most valuable assets.

According to intellectual property advisory Ocean Tomo, as of 2021 intangible assets are now responsible for 90% of all business value of S&P 500 companies.

Much of this intellectual property is stored in the cloud, where it's vulnerable to cyberattacks. Nearly 30% of U.S. companies report having their intellectual property stolen by a Chinese counterpart within the past 10 years.[8]

→ **Ethics hotlines are growing in popularity. They provide an accessible way for employees to report potential wrongdoing, possibly illegal, unethical, or improper conduct; which means a company can better protect itself from fraud, learn of employee misconduct and proactively mitigate any corruption-related risk. Any organisation, despite industry or size, should be 110% committed to having an open dialogue on ethical dilemmas regardless. Explore our "Ethics and Compliance Hotline: your frequently asked questions answered..." article for more information.**

READ MORE

LOST REVENUE:

One of the worst outcomes of a cyberattack is a sudden drop in revenue, as cautious customers move elsewhere to protect themselves against cybercrime. Companies can also lose money to hackers who try to extort their victims; in 2014 Sony came under attack by hackers as it prepared to release a comedy "The Interview."

Hackers pilfered sensitive information, including embarrassing e-mails and performance evaluations from members of the movie staff. North Korea is widely believed to be behind the attack, as the satire depicted an assassination attempt on North Korean leader Kim Jong Un.

Sony pulled the movie and released it online, and according to the National Association of Theater Owners this move cost the studio $30 million.

CYBERCRIME & REGULATIONS

The risk of cybercrime is extremely prominent; its frequency and the losses that it causes can be huge,[18] and its particular characteristics render it difficult to detect, punish and prevent.[19] Yet how have regulations responded to this relatively new form of criminal conduct, and are they sufficient?

As will be demonstrated, certain forms of cybercrime require social co-operation and preventative measures to minimise the opportunities available to such offenders.

The Computer Misuse Act 1990 is the main regulative response to cybercrime in the UK. However, its outdated nature led to its amendment under the Police and Justice Act 2006.[20] It briefly states the types of cybercrime activities that are caught within the Act 21. Although some offences have been added [22] and broadened by the 2006 Act,[23] and maximum sentences have been lengthened to adopt a tougher approach to cybercrime.

Despite these amendments, the Act hardly effectively deals with cybercrime.[24] Rather, existing legislation has been extended to incorporate modern technology in the commission of traditional offences such as fraud, theft and pornographic material. For example, section 15 of the Sexual Offences Act 2003 applies to sexual offences committed via the internet, such as grooming a child for sexual activity. Section 2 of the CMA 1990 specifically provides a mechanism for applying previous legislation to crimes committed by means of such modern technology.

The extension of traditional offences to cybercrimes of the same type can be seen in various legislative provisions. The Forgery and Counterfeiting Act 1981, for example, has been applied to property theft committed online[25], and the Theft Act 1968 has also been amended to include transfers by deception.[26]

The latter amendment responds to the increasing number of phishing offences that characteristically involve money transfer. However, these sections have been repealed by the Fraud Act 2006, which classes certain fraudulent activities as cybercrime if they are committed wholly or partly online.[27] It is clear that previous legislation, despite such extensions to cybercrime, struggles to keep up with and apply effectively to modern technology.[28]

Some have indeed suggested that the huge increase in cybercriminal activities results from insufficient and outdated legislation, which does little to hinder such offenders.[29]

The borderless nature of cybercrime has also led to conclusions that global attempts should be formulated to

eradicate the problems posed by cross-border legal operations and legislative applications.[30]

The Cybercrime Convention, for example, seeks to formulate a framework geared toward the facilitation of cross-border attempts to combat cybercrime.[31]

The Convention promotes the establishment of common policies by providing a framework for harmonising international legislation and facilitating international cooperation.[32] The international reach[33] of this Convention is advantageous in aiding attempts to combat cybercrime without hindrances posed by cross-border investigations and convictions.[34]

With such a range of activities being pursued with such inventiveness, the response of Europol and its partners must itself be comprehensive, dynamic and relentlessly innovative. And it is.

First, there's the institutional response. In 2013 Europol set up the European Cybercrime Centre (EC3) to bolster law enforcement's response to cybercrime in the EU and help protect European citizens, businesses, and governments.

Each year the EC3 issues the aforementioned Internet Organised Crime Threat Assessment (IOCTA), which sets priorities for the EMPACT Operational Action Plan in the areas of cybercrime that are the focus for that year. The EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT).

Its mission is to drive intelligence-led, coordinated action against key cybercrime threats through cross-border investigations and operations by its partners.

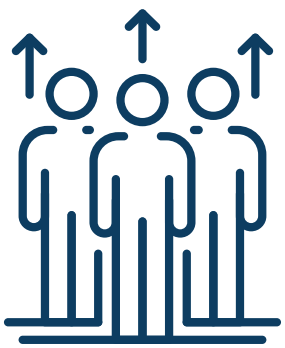
These institutional arrangements have led to notable successes at the operational level, including:

- the coordination of a joint operation, including private-sector partners to target a botnet, Ramnit, that had infected millions of computers around the world;
- coordination with Eurojust in an operation targeting large-scale malware attacks that originated in Ukraine and that were being investigated by a number of agencies — an operation that led to tens of arrests and continues to supply evidence that supports other cybercrime investigations;
- an operation targeting a major cybercriminal forum engaged in trading hacking expertise, malware and botnets, Zero Day Exploits, access to compromised servers, and matching partners for spam campaigns and malware attacks.

YOUR RESPONSE AS A BUSINESS MATTERS

HOW CAN YOU PROTECT YOUR BUSINESS FROM CYBERCRIME?

SAFE TELEWORKING TIPS AND ADVICE:
Since teleworking has become a way of life for many people, Europol has published these tips for keeping a safe remote working environment for both employees and businesses:



FOR EMPLOYEES

- Access company data with corporate equipment
- Use secure remote access
- Keep business and leisure apart
- Avoid giving out personal information
- Think before connecting
- Protect your teleworking equipment and environment
- Stay alert
- Report suspicious activity
- Develop new routines
- Be careful when using private devices for telework

FOR BUSINESSES

- Establish corporate policies and procedures
- Secure your teleworking equipment
- Secure your corporate communications
- Raise staff awareness about the risks of teleworking
- Regularly check in with staff
- Provide secure remote access
- Keep device operating systems and apps updated
- Increase your security monitoring

CHALLENGES WITH REPORTING HINDER THE ABILITY TO CREATE AN ACCURATE OVERVIEW OF CRIME PREVALENCE, BUT...

The huge risks posed by cybercrime are quite simply difficult to overexaggerate and ignore.

The cybercriminal can now commit his crimes with relatively little effort through a computer and Internet Service Provider (ISP). As has been demonstrated, old terminology contained in legislation struggles when extended to include modern cybercrime.

This disadvantage, coupled with the difficulties in locating such criminals and the damaging effects that such crimes can have, reveals that the risks of cybercrime require more rigorous action. And COVID-19 only highlighted criminal opportunism.

Despite regulatory efforts, it is clear that an anti-cybercrime culture must be implemented that promotes greater security, closer protection of privacy and awareness of potential threats to the public.[35] And unfortunately, the continued challenges with reporting hinder the ability to create an accurate overview of crime prevalence across the EU.

A lack of care or security provides the very opportunities that cybercriminals seek. With cryptocurrencies continuing to facilitate payments for various forms of cybercrime, there is a need for new developments with respect to privacy oriented crypto coins and services in order to put a stop to cybercrime.

The spread of disinformation enhances cybercrime opportunities. The need to adopt an international approach to combatting cybercrime arguably begins with the individual's use of technology.

THE TIME TO ACT IS NOW

Cybercrime has firmly entrenched itself as a part of our modern, device-driven world, and it will only continue to increase in the coming years and decades.

As government leaders work to pass new laws and update existing ones to counter the threat posed by cybercriminals, businesses must be vigilant and proactive in taking their own steps to protect their own investments – and their customers' data.

An unprotected or poorly protected company is nothing more than an easy mark for today's cybercriminals. Reach out to the experts to minimize your risk today, and be better protected against cybercrime tomorrow.

LET'S TALK!

HAVE YOU TAKEN "REASONABLE CARE" TO AVOID HARM TO YOUR BUSINESS?

Due Diligence on potential business partners, when adding a new vendor or even when hiring a new employee is vital to confirm legitimacy and reduce the risks associated with such professional relationships.

Global integrity due diligence investigations provide your business with the critical information it needs in making sound decisions regarding mergers and acquisitions, strategic partnerships and the selection of vendors and suppliers. The level of due diligence will ensure that working with a potential i.e. trade partner will ultimately achieve your organisation's strategic and financial goals.

Operating in the international market requires organisations to establish partnerships with numerous third parties, which supply raw materials, run business operations abroad and/or act as agents. At the same time, third parties are considered as the greatest area of bribery risks for international enterprises. **Under the Bribery Act 2010, British-based organisations have to conduct due diligence on their third parties as the core principle of meeting the adequate procedures requirement.**

GET A FREE QUOTE NOW!

HOW IT WORKS?

Use our DueDiligence360™ reports to help you **comply** with anti-money laundering, anti-bribery, and corruption regulations or ahead of a merger, acquisition, or joint venture. You can also use them for third-party risk assessment, onboarding decision-making, and identifying beneficial ownership structures.

Identify key risk issues clearly and concisely using accurate information in a well-structured and transparent report format. Our comprehensive range of reports includes specialised reports that support specific compliance requirements.

Protect your reputation and the risk of financial damage and regulator action using our detailed reports. They enhance your knowledge and understanding of customer, supplier, and third-party risk, helping you avoid those involved with financial crime.

FULL BROCHURE HERE!

REFERENCES

Books & Journals

Armstrong, HL & PJ Forde, 'Internet Anonymity Practices in Computer Crime'
(2003) 11 Information Management & Computer Security 5.

Athanasopoulos, E., A Makridakis, S Antonatos, D Antoniades, S Ioannidis, KG
Anagnostakis & EP Markatos, 'Antisocial Networks: Turning a Social Network into a
Botnet' (2008) 12 Information Security 146.

Brenner, SW., 'Is there such a thing as "Virtual Crime"?' (2001) 4 California Criminal Law Review 1.

Brenner, SW & JJ Schwerha, 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime' (2002) 20 Journal of Marshall J Computer &
Information Law 347.

Brenner, SW., 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 Virginia
Journal Of Law and Technology 13.

Chik, WB & W Bartholomew, 'Challenges to Criminal Law Making in the New
Global Information Society: A Critical Comparative Study of the Adequacies of
Computer-Related Criminal Legislation in the United States, the United Kingdom
and Singapore', Cybercrime and the Law (Icfai Law Books), 2007.

Clough, J., Principles of Cybercrime, Cambridge University Press, Cambridge,
2010.

Csonka, P., 'The Council of Europe Convention on Cyber-Crime: A Response to the
Challenge of the New Age' in R Broadhurst & P Grabosky (eds.), Cyber-Crime: The
Challenge in Asia, Hong Kong University Press, Hong Kong, 2005.

Dibbell, J., 'My Dinner with Catherine MacKinnon and Other Hazards of Theorizing
Virtual Rape', 2013. Source: http:www.juliandibbell.com/texts/mydinner.html,
Accessed: 14.11.2013.

Edwards, L., 'Dawn of the Death of Distributed Denial of Service: How to Kill Zombies' (2006) 24 Cardozo Arts & Entertainment Law Journal 23.

Fafinski, S., 'Computer Misuse: The Implications of the Police and Justice Act
2006' (2008) 72 Journal of Criminal Law 1.

Fletcher, N., 'Challenges for Regulating Financial Fraud in Cyberspace' (2007) 14
Journal of Financial Crime 2.

Holeton, R., Composing Cyberspace: Identity, Community, and Knowledge in the
Electronic Age, McGraw-Hill, Boston, 1998.

Hunton, P., 'The Stage of Cybercrime Investigations: Bridging the Gap Between
Technology Examination and Law Enforcement Investigation' (2011) 27 Computer
Law & Security Review 1.

Loader, BD & D Thomas, Cybercrime: Security and surveillance in the information
age, Routledge, Oxon, 2013.

Savirimuthu, A & J Savirimuthu, 'Identity Theft and Systems Theory: The Fraud Act
2006 in Perspective' (2007) 4 SCRIPTed Journal of Law, Technology & Society 4.

Smith, RG., P Grabosky & G Urbas, Cyber Criminals on Trial, Cambridge University
Press, Cambridge, 2004.

Soma, JT., TF Muther & HML Brissette, 'Transnational Extradition for Computer
Crimes: Are New Treaties and Laws Needed?' (1997) 34 Harvard Journal on Legislation 317.

Sommer, P., 'The Future for the Policing of Cybercrime' (2004) 4 Computer Fraud
& Security 1.

Sprinkel, SC., 'Global Internet Regulation: The Computer Virus and the Draft Convention on Cyber-Crime' (2002) 25 Suffolk Transnational Law Review 491.

Sussman, MA., 'The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium' (1999) 9 Duke Journal of Comparative &
International Law 451.

Tuluc, AM., 'Economic Processes Associated with the Cybercrime Industry' (2012)
2 Economics, Management, and Financial Markets 179.

Wall, DS., Cybercrimes: The Transformation of Crime in the Information Age, Polity,
Cambridge, 2007.

Wall, DS., 'Cybercrime and the Culture of Fear: Social Science Fiction(s) and the
Production of Knowledge about Cybercrime' (2011) 11 Information, Communication & Society 6.

Yar, M., Cybercrime and Society, 2nd edn, Sage, London, 2013.

-

FBI, Crime in the United States: Section V –Special Report, Bank Robbery in the
United States, 2002. Source: http://www.fbi.gov/about-us/cjis/ucr/crime-in-theu.s/2002, Accessed: 14.11.2013.

House of Lords Science and Technology Committee, Personal Internet Security:
Fifth report of Session 2006-07, Stationery Office, London, 2007.

International Telecommunications Union, 'Global Cybersecurity Agenda: High-Level
Experts Group, Global Strategic Report', 2008, Source: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html, Accessed: 14.11.2013.

Case Law

R v Gold & Schifreen (1988) AC 1063.

WHY CRI GROUP?

Since 1990, Corporate Research and Investigations Limited “CRI Group” has safeguarded businesses from fraud and corruption, providing insurance fraud investigations, employee background screening, investigative due diligence, third-party risk management, compliance and other professional investigative research services. CRI Group’s expertise will add to the diverse pool of business support services available within your region.

INVESTIGATIVE RESEARCH

ANTI-CORRUPTION & REGULATORY INVESTIGATIONS
ASSET SEARCH & RECOVERY
FRAUD RISK & INSURANCE INVESTIGATIONS
IP INFRINGEMENT INVESTIGATIONS
INTERNAL INVESTIGATIONS & CONFLICT OF INTEREST
FINANCIAL INVESTIGATIONS & FORENSIC ACCOUNTING

BUSINESS INTELLIGENCE

MARKET RESEARCH & ANALYSIS
COMMERCIAL INVESTIGATIONS

COMPLIANCE SOLUTIONS

INVESTIGATIVE DUE DILIGENCE
CORPORATE SECURITY & RESILIENCE
THIRD-PARTY RISK ASSESSMENT
ANTI-MONEY LAUNDERING
INTEGRITY DUE DILIGENCE

DueDiligence360™
Partners to TRUST

BACKGROUND INVESTIGATIONS

VENDOR & 3RD PARTY SCREENING
PERSONNEL VETTING & PRE- EMPLOYMENT SCREENING
EMPLOYEE INTEGRITY DUE DILIGENCE

EMPLOYSMART™
Smarter Background Checks Today for a Better Workforce Tomorrow

CERTIFICATION & TRAINING

ISO 37001 ANTI-BRIBERY & ANTI-CORRUPTION MANAGEMENT SYSTEMS
ISO 37301 COMPLIANCE MANAGEMENT SYSTEMS
ISO 31000 RISK MANAGEMENT SYSTEMS
ISO 37002 WHISTLEBLOWING MANAGEMENT SYSTEMS UNDER DEVELOPMENT
ISO 37000 GUIDANCE FOR THE GOVERNANCE OF ORGANISATIONS UNDER DEVELOPMENT

ABAC ANTI-BRIBERY ANTI-CORRUPTION CENTER OF EXCELLENCE

WHY WORK WITH US?

- CRI Group has one of the largest, most experienced and best-trained integrity due diligence teams in the world.
- We have a flat structure which means that you will have direct access to senior members of staff throughout the due diligence process.
- Our multi-lingual teams have conducted assignments on thousands of subjects in over 80 countries, and we’re committed to maintaining and constantly evolving our global network.
- Our solutions are easily customisable, flexible and we will tailor our scope to address your concerns and risk areas; saving you time and money.
- Our team of more than 50 full-time analysts is spread across Europe, Middle East, Asia, North and South America and is fully equiped with the local knowledge to serve your needs globally.
- Our extensive solutions include due diligence, employee pre & post background screening, business intelligence and compliance, facilitating any decision-making across your business no matter what area or department.

Zafar I. Anjum, Group Chief Executive Officer
e: zanjum@CRIgroup.com | **t:** +971 50 9038184
Zafar, Group CEO of Corporate Research and Investigations Limited (CRI Group), has been building a 30 years' career in the areas of anti-corruption, fraud prevention, protective integrity, security, and compliance. Possessing both industry expertise and an extensive educational background (MS, MSc, CFE, CII, CIS, MICA, Int. Dip. (Fin. Crime), CII, MIPI, MABI), Zafar Anjum is often the first certified global investigator on the scene when multi-national EMEA corporations seek to close compliance or security gaps.

Global Leader in Risk Management, Background Screening and Due Diligence Solutions

37th Floor, 1 Canada Square,
Canary Wharf,
London, E14 5AA,
United Kingdom
t: +44 203 927 5250
e: london@CRIgroup.com

LET'S TALK

If you'd like to discuss your business needs, we'd love to hear from you.

EMEA HEAD OFFICE
United Kingdom
Corporate Research & Investigations Ltd.
37th Floor, 1 Canada Square,
Canary Wharf, London, E14 5AA,
United Kingdom
t: +44 203 927 5250
e: london@crigroup.com

MIDDLE EAST
UAE — Dubai
Corporate Research & Investigations Ltd.
917, Liberty House, DIFC P.O. Box 111794,
Dubai, U.A.E.
t: +971 4 3589884 | +971 4 3588577
toll free: +971 800 274552
e: cridxb@crigroup.com

UAE — Abu Dhabi
Corporate Research & Investigations Ltd.
Office No: 3509, 35th Floor Al Maqam Tower, ADGM Square, Al Maryah Island, Abu Dhabi, U.A.E
t: +971 2 4187568
e: criadgm@crigroup.com

Qatar
Corporate Research & Investigations LLC — QFC Branch
Office No. 130, 1st Floor, Al – Jaidah Square,
63 Airport Road, PO Box: 24369, Doha, Qatar
t: +974 4426 7339 | +974 7406 6572
e: doha@crigroup.com

NORTH AMERICA
U.S.A.
Corporate Research & Investigations LLC
445 Park Avenue, 9th Floor New York,
NY 10022, United States of America
t: +1 212 745 1148
e: newyork@crigroup.com

Canada
Corporate Research & Investigations Ltd.
540, 439 University Avenue,
5th floor Toronto ON, M5g 1Y8, Canada
t: +1 437 836 3223
e: toronto@crigroup.com

SOUTH AMERICA
Brazil
Corporate Research & Investigations LLC
Paulista Building 2064/2086 Paulista Avenue,
14th floor, São Paulo 01310-928 Brazil
t: +55 11 2844 4290
e: brazil@crigroup.com

ASIA
Malaysia
Corporate Research & Investigations LLC
Lot 2-2, Level 2, Tower B, The Troika,
19 Persiaran KLCCM, 50450 Kuala Lumpur, Malaysia
t: +60 32178 6133
e: malaysia@crigroup.com

Singapore
Corporate Research & Investigations (Pte.) Ltd.
1 Raffles Place, #19-07, Tower 2, One Raffles Place,
Singapore 048616
t: +65 9723 5104
e: singapore@crigroup.com

Pakistan — Islamabad
Corporate Research & Investigations (Pvt.) Ltd.
Level 12, #1210,1211, 55-B, Pakistan Stock Exchange (PSE) Towers, Jinnah Avenue,
Blue Area, Islamabad, Pakistan
toll free: +92 (51) 080 000 274
t: +92 (51) 111 888 400
e: pakistan@crigroup.com

Pakistan — Karachi
Corporate Research & Investigations (Pvt.) Ltd.
BRR Towers 13th Floor, I.I Chundrigar Road,
Karachi 74000 Pakistan
t: +92 (51) 111 888 400
e: pakistan@crigroup.com

Scan & find out more about CRI Group or go to:
crigroup.com/about

info@crigroup.com