Cybersecurity

Cybercrime:
How to protect yourself and your office data

Grant Thornton | Malta

Contents

Introduction to cybercrime

Cybercrimes can be carried out by individuals, hackers' collectives, and Government agencies. While the objective of the first two groups may be gaining financial benefits by stealing and selling information, state actors aim at gathering data such as government and company records, and personal information about private citizens, which can be used for corporate and military espionage with the aim of achieving a strategic advantage over a rival nation.

In recent years, the deep web has emerged as the digital playground for criminals involved in a number of illegal transactions, which may include the sale of drugs, weapons, and information, as well as human trafficking. The deep web (estimated to be 500 times larger than the "regular" internet) can only be accessed using dedicated browsers, such as Tor. However, internet users can be targeted even while browsing the "regular" internet. These are the most common risks:

Malicious advertising: consists in tricking the user into clicking an advertisement (usually a banner) which redirects him to a website infected by a virus or malware that is automatically downloaded into the computer or mobile device (05);

Phishing: phishing is used to fraudulently obtain sensitive data such as usernames, passwords, and credit card details. Phishers use what is called "email spoofing", which consists in sending an email, apparently originated by a legitimate entity (such as a bank), to trick the recipient into opening a link which redirects him to a cloned version of a legitimate website. At this point the target is asked to provide sensitive data, such as credit card details, usernames, and passwords which will be collected by the hacker (05);

Social engineering: is a tactic used to establish direct contact with the target person through email, telephone calls, and other online communication channels. The aim is to build trust and convince the target to provide sensitive private information which can be used for fraudulent purposes (05);

Ransomware: this is a malicious software which is injected into a target computer to deny access to its user until a ransom is paid to the attacker (usually using cryptocurrencies). The average payment in 2018 amounted to $1077 per device (05, 06);

Hacking: perhaps the most common cybercrime offence. Hacking is the act of gaining illegal access to a computer, a network, or a website. The hacker can then inject viruses, delete, steal, or modify data (05).

The risks for small and medium enterprises

With most companies moving their operations partially online as a result of the COVID-19 pandemic, cybercrime increased by 600% in 2020, with 43% of the offences targeting small businesses, only 14% of which were prepared to respond to such incidents. When facing these attacks, small and medium enterprises (SMEs) have reported experiencing the following issues (2):

Inadequate security: 45% of SMEs declare that their processes are ineffective at mitigating attacks;

Heighthened frequency of attacks: 66% of companies have been targeted by a cyber attack in 2021.

The most frequent type of attacks were:

- phishing/social engineering, 57%
- compromised or stolen devices, 33%
- theft of credentials, 30%

All the above incidents can cause considerable long-term damage to an organisation, including loss of data, business disruption, revenue losses from system downtime, or even reputation damage. Whilst it is necessary for IT countermeasures to be deployed, nothing can prove more effective in closing security loopholes than adequately training employees to recognise a threat as soon as it arises.

Cybercrime in the European Union

The EU's response to online criminal activities has been to implement a specific legislation and seek operational cooperation to support member states in setting up a cyber security strategy.

To this regard, over the past two decades, the EU has implemented the following directives:

2013: a directive on attacks against information systems;

2011: a directive on fighting online sexual exploitation and child pornography;

2002: an ePrivacy directive;

2001: a Framework Decision on fighting fraud and counterfeiting of non-cash means of payment;

As of December 2018, the EU has strengthened its cybersecurity policy, after a political agreement was reached on the Cybersecurity Act (08, 09).

In 2013, Europol set up the European Cybercrime Centre (EC3) to strengthen the law enforcement response to cybercrime in the EU. Every year the centre release the Internet Organised Crime Threat Assessment (IOCTA), a strategic report on key findings and emerging threats and developments in cybercrime.

Relevant statistics

Global cybercrime damage in 2021 amounts to $16.4 billion a day, $684.9 million an hour, $11 million per minute, and $190,000 per second (6).

- A total internet shutdown would lead to a GDP loss of 1.9% daily for a country with high connectivity and a daily loss of 0.4% for a low-connectivity country (World Economic Forum, 2020);
- The likelihood of detecting and prosecuting the perpetrators of cyberattacks in the US is at a dismal 0.05% (World Economic Forum, 2020);
- 70% of cryptocurrency transactions will be connected to or used for illegal activities by 2021 (6);
- Attacks on IoT (Internet of Things) devices soared by 300% in 2019 (World Economic Forum, 2020);
- According to Comparitech's study (8), the most cyber secure countries in the world, based on cyberattack vulnerability score, are Denmark (6.72), Sweden (8.40), Germany (9.39), Ireland (9.40), and Japan (9.46);
- On the other hand, the least cyber secure countries in the world, based on cyberattack vulnerability score, are Algeria (48.99), Tajikistan (48.54), Turkmenistan (48.39), Syria (44.51), and Iran (43.48) (8);
- As of April 2021, the FBI's Cyber's Most Wanted List included 102 notorious criminals known to have committed a string of cybercrimes that have endangered and cost people and organizations billions of dollars (FBI, 2021);
- 16% of organizations received more than 100,000 daily security alerts in 2020 (Cisco, 2020);
- The top 5 worst crypto hacks are Coincheck ($500 million, 2018), Mt. Gox ($460 million, 2011), Bitfinex ($72 million, 2015), Binance ($40 million, 2019), and Bittrex ($18 million, 2018) (Coin Insider, 2021);
- The global industries most frequently targeted by cyberespionage based on the number of incidents in 2019 are manufacturing (75), professional (40), public (26), information (11), and mining and utilities (6) (Verizon, 2020);
- 89% of executive leaders consider cybersecurity a high priority (Cisco, 2020);
- In the information industry, web application cyberattacks account for 40% of data breaches (Verizon, 2020);
- The most common hacking variety in the manufacturing sector is the use of stolen credit cards, accounting for around 80% of hacking-related breaches (Verizon, 2020);
- In 2019, a 78% increase in supply chain cyberattacks, and a 48% increase in attacks involving malicious email attachments via Office files have been recorded. (Symantec, 2019);
- 86% of data breaches across all industries are financially motivated (Verizon, 2020).

How to protect yourself

Although it will never be possible to completely avoid being targeted by hackers, it is nonetheless important to mitigate the risk of an attack. The following are some useful precautions one can take.

Choose robust passwords

The most common (and weakest) passwords are “123456” and “password” as well as birth dates. Passwords should include at least 10 or more characters, with at least one uppercase letter, one lowercase letter, one symbol, and one number. It is also necessary to use different passwords for each platform and to change them at least every 60 to 120 days (12).

Regularly backup your data

A safe way to back up data is by using the 3-2-1 Backup Rule. This is a common approach whereby the data is saved and copied in 3 different platforms, 2 of which are on different devices or media storage, with 1 copy stored on an offset location or in a cloud (12,13).

Update your operating system and software

It is crucial to update operating systems and software when required, as these updates often come with the latest security patches (12).

Case study: the Bank of Valletta money heist (2019)

On February 13, 2019, hackers broke into Bank of Valletta’s system (BOV) and transferred €13 million to several foreign accounts.

The breach was discovered after 30 minutes, and the bank enforced a security lockdown, stopping all BOV-operated point-of-sale process card payments and preventing ATMs from dispensing currency.

BOV resumed its operations the following day, confirming that no ATMs, cards and client records had been tempered with. The hackers managed to transfer the money to banks in the UK, US, Czech Republic and Hong Kong.

As of September 2019, €10 million (out of the 13 stolen) have been recovered (17,18,19,20).

Case study: the Sony Pictures hack (2014)

On November 24, 2014, Sony Pictures was hacked by a group called “The Guardians of Peace”.

The hack involved stealing large amounts of information, including email communications between employees. The company’s network was also down for days, as Sony struggled to fix security-related issues.

It is widely believed that the attack was carried out by Bureau 121, North Korea’s cyberwarfare unit, under direct orders from Kim Jong Un, who was being ridiculed by a movie produced by Sony Pictures and in the process of being distributed in cinemas worldwide. Sony ultimately decided to suspend the distribution of the movie (03, 04).

Install an antivirus software

An antivirus software does not only detect any viruses downloaded on a device, but it can also warn the user about suspicious email attachments and unsafe websites. It has to be noted how a number of fake antivirus software (containing viruses or malwares) can be found online. It is therefore necessary, to download software from trustworthy websites only (15).

Visit secure websites only

Make sure that you only visit websites whose address starts with "https" instead of simply "http". The "s" means that the website is safe, as it uses a HyperText Transfer Protocol Secure which, among other things, allows for the exchange of encrypted information with the user (16).

Be cautious when connecting to public Wi-Fi networks

When a device is connected to a public Wi-Fi network, nearby devices which are on the same network may be able to intercept data. Therefore, one should only use a Virtual Private Network (VPN) which creates a safe and encrypted connection (14).

Carry out a vulnerability assessment

A vulnerability assessment can only be carried out by IT professionals. These specialists will examine a network and compile a report to recommend any corrective action which may be necessary to make it safe. Vulnerability assessments should also be carried out on mobile devices and personal computers (12).

Case study: the Yahoo! data breaches (2013-2014)

In 2013, Yahoo! fell victim to one of the most extensive data breaches in history, when the personal data, passwords and emails of 3 billion users were stolen by hackers. A second attack (targeting 500 million accounts) took place in 2014. The intruders managed to steal security questions and backup emails, which are used to reset lost passwords. The information illegally obtained, was found to have been sold on the deep web (07, 10, 24,25).

Case study: the Sony Playstation Network data breach (2011)

In 2011 hackers stole the names, home addresses, emails, birthdates, usernames, passwords, logins and security questions of 77 million users of the PlayStation Network (PSN). The information was sold on the deep web for illegal purposes. As a result of the attack, Sony shut down the PSN for one week until a proper investigation could be completed by an external security firm. Further protection measures were put in place following the findings of the investigation (21,22,23).

How Grant Thornton can help keep your office data safe

Under GDPR, failing to adequately protect your customers' data can result in hefty fines. We can help.

Grant Thornton operates a team of qualified cybersecurity experts, who can carry out a full vulnerability audit of your business and provide you with solutions to ensure that your corporate and customer data is adequately protected against internal and external threats. Get in touch now with one of our experts to find out how we can help you secure your office data.

Contacts

Joseph Pullicino

Partner | IT, Business Risk & Outsourcing

T +356 9949 9660

E joe.pullicino@mt.gt.com

Chris Farrugia

Partner | Information Technology

T +356 9982 9636

E chris.farrugia@mt.gt.com

Daniel Farrugia

Senior Manager | IT & Business Risk

T +356 7922 7962

E daniel.farrugia@mt.gt.com

Anton Micallef

Senior Manager | Business Risk & Outsourcing

T +356 9944 9454

E anton.micallef@mt.gt.com

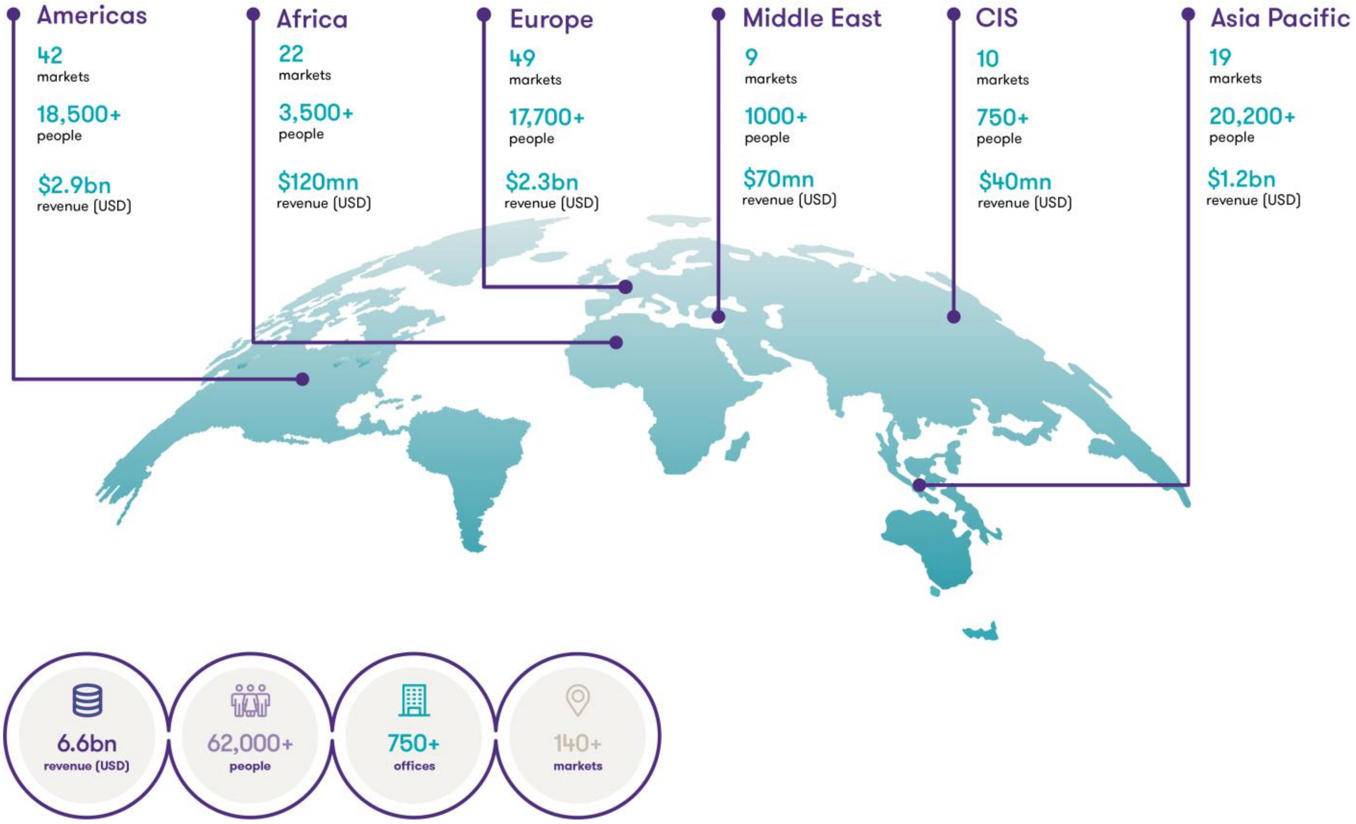
Grant Thornton International

Grant Thornton Malta is a member firm of Grant Thornton International

Grant Thornton International Ltd is a not-for-profit, non-practising, international umbrella membership entity. It is organised as a private company limited by guarantee, not having a share capital, incorporated in England and Wales and does not provide services to clients. Services are delivered independently by the Grant Thornton firms.

Grant Thornton International is an organisation of independently owned and managed accounting and consulting firms. Each member firm within Grant Thornton International is a separate national firm. These firms are not members of one international partnership or otherwise legal partners with each other, nor does membership within Grant Thornton International thereby make any firm responsible for the services or activities of any other. Each firm governs itself and handles its administrative matters on a local basis. Most of the member firms carry the Grant Thornton name, either exclusively or in their national practice names, facilitated by a name use agreement.

As of 31 December 2021 Grant Thornton had more than 62,000 people in its member firms, represented in over 140 countries. Global revenues amounted to US$ 6.6 billion.



References

1. A. (2019, March 14). *Top 5 Countries with Largest Number of Hacker.* Retrieved from Ajura: https://www.ajura.com/blog/top-5-countries-largest-number-hacker/
2. (2022, January 31). 2022 Must-Know Cyber Attack Statistics and Trends –Embroker: https://www.embroker.com/blog/cyber-attack-statistics/
3. K. Z. (2014, March 12). *SONY GOT HACKED HARD: WHAT WE KNOW AND DON'T KNOW SO FAR*. Retrieved from Wired: https://www.wired.com/2014/12/sony-hack-what-we-know/
4. Emily Todd VanDerWerff, T. B. (2015, June 3). *The 2014 Sony hacks, explained*. Retrieved from Vox: https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea
5. Hernandez, E. (2018, February 14). *The 16 Most Common Types of Cybercrime Acts*. Retrieved from VoIP Shield: https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/
6. (2022, March 1). 119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis. Retrieved from Finances Online: https://financesonline.com/cybersecurity-statistics/
7. (2017, October 3). *Yahoo 2013 data breach hit 'all three billion accounts'*. Retrieved from BBC: https://www.bbc.com/news/business-41493494
8. P.B. (2021, September 21). *Which EU Countries have the worst (and best) cybersecurity?*: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/
9. (n.d.). *Cybercrime*. Retrieved from European Commission: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en
10. N. P. (2017, October 3). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. Retrieved from The New York Times: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html?register=google
11. A. Z. (2019, May 13). *300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2019 EDITION]*. Retrieved from Comparitech: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
12. F. G. (2019, May 31). *5 simple steps to protect your office data from hackers.* Retrieved from Grant Thornton Malta: https://www.grantthornton.com.mt/insights/5-simple-steps-to-protect-your-office-data-from-hackers/
13. A. M. (2017, November 13). *The 3-2-1 Backup Rule – An Efficient Data Protection Strategy*. Retrieved from Nakivo: https://www.google.com/search?q=3-2-1+backup+rule&rlz=1C1GCEB_enMT855MT855&oq=3-2-1+back&aqs=chrome.2.0j69i57j0l4.4971j0j7&sourceid=chrome&ie=UTF-8
14. (n.d.). *11 ways to help protect yourself against cybercrime*. Retrieved from Norton by Symantec: https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html
15. (n.d.). *Cybercrime*. Retrieved from Avast: https://www.avast.com/c-cybercrime
16. L. B. (2019, February 17). *8 ways to protect yourself from cybercrime*. Retrieved from Digital Reflections: https://medium.com/digital-reflections/8-ways-to-protect-yourself-from-cybercrime-fef3eab45b9a
17. C. C. (2019, February 14). *BOV yet to establish who was behind cyberattack.* Retrieved from Times of Malta: https://timesofmalta.com/articles/view/bov-yet-to-establish-who-was-behind-cyberattack.702005
18. Bertrand Borg, V. M. (2019, February 13). *BOV goes dark after hackers go after €13m*. Retrieved from Times of Malta: https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896
19. A. G. (2019, May 9). *Remaining €2.9 million stolen in BOV cyber attack found in Hong Kong.* Retrieved from The Independent: http://www.independent.com.mt/articles/2019-05-09/local-news/Remaining-2-9-million-stolen-in-BOV-cyber-attack-found-in-Hong-Kong-6736207900
20. V. C. (2019, February 15). *BOV may not recover all money stolen by hackers*. Retrieved from Malta Chamber: https://www.maltachamber.org.mt/en/bov-may-not-recover-all-money-stolen-by-hackers
21. Ben Quinn, C. A. (2011, April 26). *PlayStation Network hackers access data of 77 million users*. Retrieved from The Guardian: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data
22. P. S. (2011, April 26). *Update on PlayStation Network and Qriocity*. Retrieved from Playstation Blog: https://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/
23. J. P. (2016, June 20). *Five years ago today, Sony admitted the great PSN hack*. Retrieved from Eurogamer: https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today
24. V. G. (2016, December 15). *Hacked Yahoo Data Is for Sale on Dark Web*. Retrieved from The New York Times: https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html
25. R. (2016, December 16). *Why Yahoo's Security Problems Are a Story of Too Little, Too Late*. Retrieved from Fortune: https://fortune.com/2016/12/19/yahoo-hack-cyber-security/

Grant Thornton