PERSPECTIVES

Cybercrime is on the rise – is your business prepared?

February 2023

This article examines the meaning of the term ‘cybercrime’ and what drives the criminals responsible. It describes, in layperson’s terms, some of the more prolific attacks that companies and individuals may suffer and highlights the importance of preparing to respond and investigate effectively.

Cybercrime – old crimes, new tools? This phrase coined in 2001 by the UK National Hi-Tech Crime Unit [1] is a play on the saying ‘old wine in a new bottle’. It covers any criminal act defined by law or civil wrongdoing perpetrated using a computer or any electronic device, on or off the internet, such as theft, fraud and blackmail. Today we have ‘new crimes, new tools’, which can only be committed by or rely upon the availability of a computer or other technology, including the internet. This includes malware and virus attacks, denial of service attacks, hacking offences and identity theft. Hence, we have the term ‘cybercrime’.

According to the US Department of Justice, all cybercrime can be organised into three categories:

- Crimes that use computers as a weapon – hacker attacks
- Crimes that target a computer or another device to gain access to a network
- Crimes where a computer is neither the facilitator nor the target but still plays an integral part in storing illegally obtained proprietary data. [2]

Relevant statistics are escalating, both in scale and in complexity. [3] Cybercrime can affect everyone, from essential services, such as a French hospital in August 2022, [4] to multinational businesses and private individuals. It causes significant network downtime, financial loss and reputational damage. [5] The rise is confirmed by figures released in August 2022 showing that 25,841 people used the Dubai Police e-crime platform on its website in 2021 to report cybercrimes. [6] The 2021 research figures from the UK technology website Comparitech support these statistics because the UAE saw a 79% rise in cybercrime reporting and a loss of $746 million. [7]

In our post-pandemic digital age, most companies conduct their business online using systems, networks, software and applications that instantly connect them anywhere. While this connectivity enables business operations globally, the increased use of connected platforms presents more significant risks than before. As technology grows and our use of it advances, so does cybercrime and the tactics criminals deploy to exploit exposed security systems and the vulnerability of users.

A key consequence of cybercrime is monetary. Cybercrime can embrace various forms of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as endeavours to misuse financial accounts, credit cards or other payment card information.

Although many law enforcement agencies worldwide have started cracking down on cybercrime, the increasing trend shows no sign of decline, especially in ransomware [8] and business email compromises (BEC). [9] Some cybercriminals now reside in countries with weak cybercrime laws. In addition, they have switched from using dollars to cryptocurrencies to avoid prosecution or having their illicit funds seized.

Notes

[1] https://www.cyber-rights.org/documents/ncis_1801.htm
[2] https://www.techtarget.com/searchsecurity/definition/cybercrime
[3] https://earthweb.com/cybercrime-statistics/
[4] https://www.france24.com/en/europe/20220823-cyber-attackers-disrupt-services-at-french-hospital-demand-10-million-ransom
[5] https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
[6] https://www.thenationalnews.com/uae/2022/08/24/more-than-25000-cybercrimes-reported-last-year-say-dubai-police/
[7] https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/
[8] https://www.expresscomputer.in/news/why-are-ransomware-attacks-increasing-these-days/88768/
[9] https://threatpost.com/fbi-bec-43b/179539/

As cited above, there are numerous diverse types of cybercrime. Most cybercrimes are carried out with the anticipation of financial gain by the perpetrators. Some common varieties of cybercrime include the following:

Ransomware

This malicious software locks the victim from their computer or blocks access to the files stored on their hard drive. Since 2013, ransomware has cost businesses and institutions billions of dollars in lost revenue. Criminals will demand bitcoin or other crypto payments to unlock the computer system.

While the significance of cyber security grows, many are still unaware of measures they can implement and actions they can take to mitigate risk, combat cybercrime and protect their future. The reality is that the best way for businesses to protect themselves against cybercrime is to invest in cyber security and understand how new tools can combat new and old crimes.

Business email compromise

BEC is a form of email fraud where employees with access to company finances are tricked into making money transfers or sharing information by email pretending to be from the CEO or a trusted customer. This cybercrime can cause substantial financial damage to a company. Investigators and lawyers must work closely with businesses to quickly assess the situation and provide solutions.

Phishing

This type of cybercrime is prevalent. Email fraud is the intentional deception made for personal gain or damage to another individual through email. Almost as soon as email became widely used, it began to be used as a means to defraud people.

Email solicitations to purchase goods or services may be instances of attempted fraud. The fraudulent offer typically features a popular item or service at a drastically reduced price – too good to be true…

Identity theft

A cybercrime often occurs when an attacker accesses a computer to gather a user's personal information. They then use the information to steal that person's identity or access their personally identifiable information (PII). Cybercriminals typically buy and sell PII on Darknet [10] markets or use it to facilitate a cybercrime or another intelligence-gathering enterprise.

With the increasing number of online criminal activities, new cybercrime models can be found in the tech news almost daily. Computers and the internet have fundamentally changed how we interconnect, participate in business, act and work with the rest of the world. The benefits of these technologies are substantial, though they also create a range of threats.

The precise effect and cost of cybercrime on companies are challenging to assess. While financial losses due to cybercrime can be noteworthy, businesses can also suffer other collateral consequences because of cybercrime, including but not limited to the following:

- Anyone can fall victim to cybercrime, and the fact that we are all virtually connected puts us at an even greater risk.
- Harm to stakeholder perception after a cybercrime can cause a company's worth to decline.
- In addition to a drop in share price, businesses that have been victims of cybercrime, particularly when avoidable, may also face higher borrowing charges and greater scrutiny when attempting to raise capital.
- Loss of confidential and sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data.
- Damaged brand identity and loss of reputation after a cybercrime dents customers' trust in a company and that company's capability to keep their data safe. Following a cybercrime, companies lose existing customers and the capacity to gain new customers is often reduced.
- Companies could also sustain direct outlays from cybercrime, including amplified insurance premium expenditure. Bringing in cybercrime experts to conduct proactive and reactive incident response and remediation, public relation preparation and other services related to cybercrime could make them a target of opportunity and not a target of choice.

Note

[10] Darknet, a computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing

Considering the economic sums and insignificant totals recovered from these cases, it is not difficult to see why criminals are surveying the cybercrime marketplace. With such vast gains and reduced risk, it is often advantageous to become a cybercriminal, resulting in a lose-lose situation for the victims.

In conclusion, since multiple forms of cybercrime have been observed for more than 25 years [11], it is unlikely that they will ever cease due to legislative, policing or jurisdictional efforts. Cybercriminals are like businesspeople – they want to make money. Therefore, is there greater value in considering how their tools and platforms can be controlled or monitored? Or, due to the rise of such cybercrimes happening regularly, should awareness training and campaigns be increased to educate more and more people to be safe from cybercrime? Lt Gen Dhahi Khalfan Tamim of Dubai Police recently stated: 'We need to prepare and qualify a generation that is capable of not only detecting these crimes and presenting undisputed evidence but also skilful enough to stop these crimes before they happen.' [12]

Notes

[11] https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

[12] https://www.thenationalnews.com/uae/2022/10/27/dubai-security-chief-warns-of-need-to-tackle-cyber-crime/

Contacts

Darren Mullins
Partner
darren.mullins@accuracy.com
+971 56 682 5681

Paul Wright
Senior Adviser
paul.wright@accuracy.com
+971 522 449429

Arthur Couvreur
Director
arthur.couvreur@accuracy.com
+33 6 66 69 65 15

Steve Molloy
Director
steve.molloy@accuracy.com
+39 334 10 49 578

Accuracy partners and professionals are available to discuss your needs and design an appropriate solution with the relevant experts.