Note: Below are extracts from an article published by The Irish Times (25th August 2023) and as referenced below.

Everyone at risk from cybercrime.

According to The Irish Times, McCall (2023) , individuals, companies and organisations are all increasingly vulnerable to cyber-attack and no one entity can escape that eventuality, no matter the size or profile:

> When it comes to cybercrime, it really is the case that no one is safe. From the individual receiving a smishing message on their smartphone asking them to click on a link to unlock their credit card to the large public service organisation being effectively shut down by a ransomware attack, no one can truly consider themselves safe or less susceptible to attacks. Criminals still follow the money, of course, and financial services organisations are still favoured targets.
>
> "Historically, financial services and healthcare have been the sectors most targeted by cyber criminals," says Aanand Venkatramanan, head of ETF EMEA at LGIM. "However, digitalisation is increasing across all industries, leading to a rising number of attacks across sectors and countries. Every individual, enterprise and organisation that has data is at risk from cybercrime." Rida Villanueva director of cybersecurity and forensics with Grant Thornton agrees. "Nearly everyone is at risk – individuals, government organisations, and private companies are all subject to attack. It's not a matter of who but when. You are at risk and will be compromised at some point. I'm sorry to deliver that message."
>
> McCall (2023)

McCall (2023) in his Irish Times article reports that particular sectors of industry are more susceptible to attack, such as Financial Services, where criminals know significant money circulates. Other sectors like government bodies and public utilities are also a target (which we have seen in recent times), where maximum disruption can often result in perceived success for the criminal. But such industries also employ the best cyber security techniques, advisors and defenses, which can deter the criminals:

> That message is echoed by Marc Roche, associate director with Accenture in Ireland's security practice. "It goes without saying that the financial sector is most at risk, but in general they also have more resources available to protect their key systems," he says. "Critical national infrastructure like electricity, water, railways, and so on, are also areas that need to be heavily protected given the potential impact to people and organisations."
>
> The criminals can be quite discerning, however. "Like most criminal activities, if you look at where the money is, then you can be assured those organisations will be on the watch list of criminals," Roche adds. "There is an inflection point though, as too much publicity can also be a negative, so most criminals want to target organisations that will be willing to pay or have something worth selling. A large attack comes with a lot of pressure for the authorities to act."
>
> McCall (2023)

McCall (2023) reminds us that cyber criminals are no different to other types of criminal. Opportunistic, with minimum effort and maximum reward, and just because your business may be relatively small and not in the public eye, this McCall(2023) Irish Times article suggests that unfortunately, there is no one individual or organisation safe from cyber-attack. The question for business owners is at what point a cyber-attack will cause the most damage and can it implement a cyber security plan to match? :

> There is nothing particularly special about cybercriminals other than their tools and methods." Cybercriminals are like any other type of criminal," says BDO director Eoghan Daly. They want to make money with the least risk and effort possible. "Cybercriminals might actively target an organisation based on an assessment of its propensity to pay a ransom, which will depend on the nature of the organisation, its activities, and how wealthy it is."
>
> Every sector is at risk to some extent, and the risk will vary within a sector, he adds. "Irish companies should consider what type of cyber incident would cause them the most problems and then prioritise their cybersecurity activities accordingly. "Would the loss of a key system stop the organisation in its tracks? Would the leaking of confidential customer information undermine consumer confidence and lead their customers to do their business elsewhere? Would a breach result in cancelled contracts?"
>
> Companies can inadvertently place themselves at higher risk of cyberattack, according to David McNamara, chief executive of cybersecurity firm Commsec. "If a cybercriminal is targeting the energy sector, for example, they will look to see who is supplying energy to certain companies. They can find that information on the internet with energy companies announcing new deals. You should be very careful about what you put not only on social media but into the mainstream media as well."
>
> Sean Morris, chief technical officer at Galway-based cybersecurity firm TitanHQ, has bad news for organisations which may believe they are too small or insignificant to attract the attention of the criminals. "There has been an awful lot of research and reporting on this," he says. "When you condense it down, there is definitely a variation between sectors but is any sector particularly at risk? The answer is no. You can look at it in terms of scale. Small businesses consider themselves low risk. Security through obscurity if you like, but large businesses invest more in cybersecurity.

“The reality is that all businesses are at risk. It doesn’t matter if it’s non-profit, a charity or a major corporation, the criminals don’t care what business you’re in. They find opportunities, exploit them, and take what they can get. That’s not a cheerful message.”

The very nature of cybercrime lends itself to widespread activity.

“Many cybercriminals use the so-called ‘spray and pray’ approach in a bid to get data or money from individuals,” says Roche. “There has been a sharp increase in these type of scam emails and SMS messages of late, and they still catch a few people out, hence why the scammers keep sending them. There will always be an opportunistic element to cyberattacks, but most cybercriminals will also have a target list containing multiple organisations and CEOs, CFOs . . . If these bad actors find an open door, they will take the time to look around and see how they could best take advantage. "

“You can buy data online and get 10,000 or 100,000 email addresses at quite a low cost,” adds Morris. “You only have to get a small percentage of those to make it worthwhile. There are so many options for cybercriminals. They don’t stand still. Some of the most innovative and resourceful people on the planet are involved in it. They do a lot of re-use and sharing with each other, and they are outstanding at finding new vulnerabilities.”

And they don’t even need to be very technologically adept, according to Villanueva who points to a fairly recent concept known as ransomware as a service. “It is now being used quite widely,” she says.” There are criminals whose job is to develop and enhance ransomware and sell and license it to other criminals as a service. You don’t have to be experts in this to deliver a damaging payload. You just have to know who to target. The more available these things are, the more susceptible everyone is.”

McCall (2023)

References

McCall, B. (2023) ‘Everyone at risk from cybercrime’, *Irish Times*, 25 August. Available at: https://www.irishtimes.com/special-reports/2022/08/25/everyone-at-risk-from-cybercrime/ . (Accessed 01 September 2023).

THE IRISH TIMES