Cyber Security A SPECIAL 2-PAGE REPORT

Striving to always stay secure in a dangerous landscape

The threat landscape is continually evolving, and small and medium enterprises are now in the firing line, writes **Jason Walsh**

Paul Delahunty, information security officer, Stryve: 'You could attack the whole of Ireland for a few thousand euro. How many hits would you get from that? Five to six million people for €2,000. You don't need a very high hit rate to make that profitable'

In the past, one approach to cybersecurity, now discredited, was 'security through obscurity'. The idea was simple, if wrongheaded: uncommon applications and systems were supposed to be less vulnerable to threats, as attackers would not understand them.

With the benefit of hindsight, we now know that there is no system so obscure that hackers can't attack it. For a start, basic principles apply to all systems but, moreover, today there is an apparently infinite amount of effort, manpower and time spent on cracking vulnerable systems and devices.

Another form of obscurity is still held out, also falsely, as a reason to take security less seriously: small size.

Worn as a kind of comfort blanket, whether it is Ireland itself being small or businesses being small, the idea goes that hackers have bigger fish to fry.

Paul Delahunty, information security officer at Stryve, said that criminals are quite happy to fry fish of any size.

"We've had a lot of talk about ransomware in the last two years, but the targets have mostly been larger businesses, but I think over the last 18 months it's starting to hit SMEs a lot harder for a number of reasons," he said.

One reason is that larger organisations are taking the threat very seriously.

"They have woken up to it and have the resources to deal with it, such as back-ups that cannot be changed, and artificial intelligence actively monitoring and fighting as the event is happening," he said.

By comparison, SMEs are a soft target. In addition, cyber-crime-as-a-service is now out there on the so-called 'dark web', Delahunty said.

"If you couple that with the fact that there is ransomware as a service, malware as a service and DDoS as a service you can see what is happening," he said.

"It's so cheap. You could attack the whole of Ireland for a few thousand euro. How many hits would you get from that? Five to six million people for €2,000. You don't need a very high hit rate to make that profitable."

In addition, Ireland is not actually small. It may be geographically small and have a small population, but it is also home to major industries including information technology, financial services and pharma.

The current environment is dominated, of course, by Russia's invasion of Ukraine, and Delahunty said this geopolitical instability brought a cyber threat in its wake.

"With the invasion of Ukraine, we can see the knock on the door happening," he said.

The business of business

The global skills shortage in cyber security is now well known, but it is also getting worse: a global workforce gap of more than 2.72 million positions has now been reported. According to the 2021 ISC 2 Cybersecurity Workforce Study, the global cybersecurity workforce needs to grow 65 per cent to effectively defend organisations' critical assets.

The truth is, though, SMEs have never been able to hire dedicated in-house cybersecurity staff anyway, so even if a concerted effort is made to fix the cybersecurity education and training pipeline, they will still require external help.

For them, the real problem is that technology is rarely their forte at all. Unfortunately, this leads some to ignore the issue until it is too late.

Delahunty said that they should engage with a provider who can do it for them.

"You go into business to make widgets. Your expertise isn't in how to secure that business. SMEs in particular shy away from it: 'I'm not good with computers', that kind of thing. Well, I'm no expert in installing house alarms but I know I need to have one installed and how to turn it on before leaving my house," he said.

Last year's attack on the HSE certainly concentrated minds in Ireland, but Delahunty said that this kind of high-profile attack can actually obscure the gravity of the situation.

Indeed, whether under pressure from a foreign state or otherwise, the group who attacked the HSE eventually released the decryption key. This is not likely to happen to a business, so they need to be prepared, Delahunty said.

"If you hack the HSE, you create an awful lot of trouble for yourself. Even other hacking groups won't like it, as it draws too much negative attention. But if a company turning over 20 or 30 or 40 thousand gets hit, who is going to care? No one, is the answer."

> "Over the last 18 months it's starting to hit SMEs a lot harder, for a number of reasons

Taking a 'prevention, not cure' approach to cyber attacks

Proactive cyber security tactics help keep the threat at bay, writes **Jason Walsh**

Malware has become a major threat to business continuity, and hackers' current favoured tactic of encrypting files and holding them to ransom is a particularly pernicious one.

It is also more common than ever. Indeed, according to one study, ransomware attacks rose by 92.7 per cent in 2021 compared to 2020 levels – and this only counts the attacks that were actually reported.

Brendan Healy, services director at Triangle, said that this growing threat required a new approach to IT security.

"We've moved on in our offering in the market. While the market itself hasn't changed much, we've driven onwards."

Triangle's approach is to focus on providing a robust early warning system that can spot incoming attacks and neutralise them. This 'prevention is better than cure' approach allows businesses to nip threats in the bud rather than discover months after the fact that crucial business data has been rendered inaccessible.

"The last thing you want is having to ring and say, 'I can't access this file'," he said.

Triangle avoids this scenario by deploying proprietary tools within databases that scan, analyse and, most of all, automate processes.

"We build a whole automated flow to protect data and also to automate the recovery. You make a back-up of your file server and it will look for encryption or potential encryption. We take as many feeds as we can and out of that we deliver automation," he said.

Brendan Healy, services director, Triangle

"If something trips an alarm, we immediately take a snapshot of the data and then we can investigate the data, doing this offline, checking if something is a false positive or is it something more serious. If it's the latter we can decide where we want to roll back to."

Without such an early warning system, businesses can find themselves backing up data every day and week thinking that they are protected but, in reality, still left exposed.

After all, back-ups are what hackers are after.

"The back-up is the first point of attack for most hackers. This reduces your risk period from what could be two months to 24 hours," Healy said.

As a result of its expertise, Triangle has now become the only Irish Certified Recovery Partner for Dell Technologies, he said.

A newer, darker world

Cyber security has never been far from the headlines, and last year's attacks on a number of Irish higher education institutes and the HSE drove it to the front pages. Today, with war in Ukraine, there is an added instability factor.

The good news is that this at least means people are open to discussing security, said Healy.

"If you look at the events that cause attacks to increase, warfare is one of them. There is absolutely a huge increase in attacks, but there is also slightly increased information about attacks. People are willing to talk about it. That openness helps other people," he said.

Against that, there has been an exponential increase in attacks, he said.

At the end of the day, security is a process, though, and paralysis caused by analysis is something that needs to be avoided. Instead, attacks should be expected and business data prepared, sorted, protected and backed up with that in mind.

"You can never be 100 per cent secure. It really is about being able to recover. We spend a lot of time with our customers identifying the data that matters. Not every piece of data is equal, so you need first to identify what data you can't run the business without," Healy said.

Triangle's services, including hardware and software, are deployed under an operating expenditure model, something Healy said resonates well in the market.

"Otherwise, it can become very capital-intensive to get into, whereas if you do it as a service you can flex it up or down," he said.