How to prevent data leaks

Even when your data is encrypted, you're still emitting metadata. Protect it. It's important.

Every time you use your smartphone, your computer or your tablet you leave behind a trail of data.

Even if your hard data (emails, phone numbers, account numbers) is encrypted, you still scatter around a vast amount of metadata.

Metadata is often as useful as hard data. From metadata, hackers can extract a very accurate picture of who you are, what company you work for, where you are, what you regularly do, who you talk to, and when you send information.

What is metadata and why is it valuable?

Metadata is the context that exists around all digital communications – phone calls, app logins, website visits, emails and social media posts. It's the 'data around the data' so to speak, and it is all a hacker needs to 'sit on,' build a profile of you (and your company) and then launch an attack.

"Data has become a valuable business commodity that is spawning a rise in cybercrime," says Paul Jacobs, partner, head of Forensics and Investigation Services Ireland.

"Obscuring and hiding metadata is one of the growth areas in the anti-cybercrime industry," says Ethan Schmertzler, CEO of Dispel, a privacy-as-a-service (PaaS) provider.

How big is the problem?

Worldwide, cybercrime costs companies over half a trillion dollars a year and the opportunities keep getting bigger for cybercriminals.

Grant Thornton believes cybercrime costs the Irish economy €630 million a year. Traditional crimes that become 'cyber', such as welfare and tax fraud, tax filing fraud, cost €257.74m of the total.

Globally, companies spend 72 billion dollars a year trying to prevent cybercrime and data leaks.

"Cybercrime is a very profitable, low-risk business for criminals. Instead of breaking into a building and stealing something valuable, cybercriminals take high-quality data from companies and either use it or ransom it," says Ethan Schmertzler.

No company, big or small, wants to end up on the front pages of newspapers due to a data breach.

Protecting your business's data and metadata is critical.

What affordable services are available?

Schmertzler's company Dispel sells commercial and individual online privacy protection. "After two years in development for large institutional clients, Dispel's privacy-as-a-service is now publicly available. Our products don't rely on fixed infrastructure, they are built on an unattributable, multi-cloud ephemeral infrastructure."

What does that mean?

"The data we protect is constantly in motion – a moving perimeter target that hackers can't find or attack. The most important thing is to keep the data moving, never be static," says Schmertzler.

The data breach problem is growing

Eoin O'Reilly, EY Ireland's partner lead on Forensic Data Analytics (FDA), says, "The threat of cybercrime is an everyday reality, posing a dynamic and relentless challenge for organisations of all sizes.

"We are having more and more conversations with senior managers on how to incorporate FDA as a critical component of their risk management and compliance programs. This is vital given the current regulatory enforcement environment and market reaction to instances of alleged corporate fraud, bribery, and cyber breach."