Stop sweeping corporate data breaches under the rug: Interview with Nathaniel Fried, cofounder of TurgenSec

Do you really have any idea how much of your data is publicly available – legally or illegally? TurgenSec helps people and organisations get to grips with how exposed they are, before offering an across-the-board cybersecurity package to remedy this exposure.

Temps de lecture : minute

---

25 February 2021

Maddyness spoke to cofounder Nathaniel Fried about how transparency aids recovery from data breaches and stops them from happening in the future; how social media has changed everything; and his experience on the NCSC Cyber Accelerator.

[*Maddyness*] Tell me about your background leading up to the genesis of TurgenSec. Did you have expertise in this area already?

[Nathaniel] TurgenSec was founded by me and Peter Hansen. I had a small amount of experience in OSINT (open source intelligence), while Peter has years of experience.

We were swiftly joined by Dr Alex Tarter as a cofounder. He has been in the industry for many years and is the current Chief Cyber Consultant & CTO of Thales Cyber & Consulting.

How has the security landscape changed in recent years? How does TurgenSec deal with uniquely modern security challenges?

Data breaches are becoming more common due to systemic failures of basic assurance and boards not taking the risks seriously. This is extremely evident in our responsible breach disclosures. Take for example this breach, impacting almost 200 law firms including some magic circle ones that we disclosed.

Leaving a database open to public view for an extended period with thousands of legal documents shows a failure of really basic ongoing assurance practices.

> *Companies need to do a better job of managing and controlling their exposed data footprint.*

COVID has caused the attack surfaces of companies to become more disparate. Employees are working from home and providing new routes into company infrastructure for attackers. Enterprise solutions have to change to meet this new challenge as our personal online presence increasingly becomes intertwined with our business presence.

TurgenSec's Data Shadow product allows individuals to view their online presence, from data held by private companies like Facebook to breached data (and everything in between), from the perspective of an attacker and then take ownership over that data. This is a necessary step in mitigating and understanding cyber risk in this new era.

Are there industries where personal or company data is particularly threatened?

Personal data is threatened all across the spectrum. TurgenSec has disclosed serious data breaches in important sectors such as legal and medical, but most damaging from the perspective of data rights appears to be the impact on children.

For example, we recently disclosed a breach of almost one million children's personal details via a database at the Bill Gates founded charity, Get Schooled.

What effect is social media having on the security of individuals' data, and companies'

reputations? Do you have any views on how it could be better regulated?

Social media has really changed the way that people interact with the Internet and the amount of information they're willing to share both explicitly and implicitly. As that change has been so rapid, we're finding that our approaches are maturing not through considered thought, but by constant trials by fire.

> *Our private thoughts and expressions are now more public; data shared once is suddenly able to be replicated indefinitely.*

Companies realised this earlier than a lot of people, which is why there is now a whole field devoted to corporate reputation management. There are whole businesses currently devoted to protecting and managing the digital reputations of big businesses. But as we see time and again, it's not just companies who need to protect their reputations.

Your professional and social reputation impacts your daily life all the time, from your opportunity to get hired to maintaining social relationships and friendships. Your online presence is now a critical part of your personal reputation – but until now there's never been a company out there who can help individuals manage it.

What does Brexit mean for data privacy?

Luckily for most individuals not much. We are still aligned to the EU GDPR regulations which means consumers still have powerful rights they can exercise to control their online reputations and digital footprints.

Hopefully the UK will continue to build on this start, and meet its ambitions set out in the UK National Cyber Security Strategy to “build a flourishing digital society”.

I’m interested in your Intelligence Acquisition element. Do you help people expose data misuse or general wrongdoing as well?

Our Intelligence Acquisition service can help uncover both general wrongdoing and data misuse. Some common uses of our Intelligence Acquisition service:

- Unmasking the true identity of malicious actors on the deep web, selling stolen company data to inform legal action or internal investigations.
- Providing intelligence on the identities of those behind fraud marketplaces to inform legal action or internal investigations.
- Tracking the source of breached data to highlight insider threats and inform legal action or internal investigations.

What has your experience with Wayra and the NCSC been like?

Working with the NCSC and Wayra on the Cyber Accelerator has been an extraordinary experience that has given us the tools and skills to confidently lay the groundwork for raising funding.

The NCSC has offered us valuable insights and assistance with some of the complicated compliance issues we face and we look forward to a long relationship with them.

What are some of the most interesting and challenging data breaches (and solutions) you've witnessed?

The response to data breaches can be very varied and not always pleasant.

We have been personally threatened, forced into NDAs by powerful institutions and accused of all manner of outrageous things.

How should companies change their approach to avoiding and managing data breaches?

At the moment companies are still operating under a suppress and dissemble approach to data and security breaches. They typically play down the impact to their customers or those impacted and stick very much to the letter of the law.

For instance, because GDPR is at the forefront of the conversation and carries the threat of regulatory fines, most companies always lead with a statement around personal and identifiable information. But this is typically only a small percentage of the data exposed.

It would be much better if companies took a more transparent approach to reporting breaches – and helped inform people about what data was breached. This would allow for fuller assessment and mitigation. If those impacted are only told half the story, it is very difficult to assess the level of impact.

> *A responsible disclosure deals first with the harm caused to those whose details have been exposed, before shifting attention to the company impacted.*

Any company that accidentally or intentionally exposes data meant to remain private should make every effort to immediately remedy the

issue. It should make every effort to reach those impacted, inform them what information was exposed, and review their own processes to ensure that this type of breach never happens again.

Public awareness campaigns about breaches are important – especially in the cases where the people impacted may not have even realised. This is something that most companies want to avoid – but sunlight is often the best disinfectant.

And finally, a more personal question. What's your daily routine at the moment - and what are the rules you're living by to get you through COVID-19?

COVID has changed the world, and accelerated the problems our company aims to address.

Despite ruining my yearly trip to Italy for my birthday COVID has impacted my life little. I still sit at a computer for 15 hours a day.

Discover TurgenSec

Article by Florence Wildblood