



Royalty-free stock photo ID: 244628476

Mar 23, 2020 15:27 GMT

# Use it or lose it: personal data joins the list

Spectrum regulators around the world have long been big fans of the 'use it or lose it' principle when it comes to licensing radio spectrum, or specific

frequencies, particularly when that spectrum sits in a band that is in high demand. It even merits a mention in the EU's European Electronic Communications Code, due to take effect before the end of 2020.

By now, those operating in the cyber security world should have adopted their own version of the 'use it or lose it' principle, driven by the need to eliminate unnecessary risk. All unused software, and hardware services that are no longer required, should be deleted, disposed of, or turned off.

It is worth noting that a significant proportion of the cyber attacks our Cyber Incident Response Team (CIRT) respond to have occurred solely because someone with malicious intent has exploited functionality that should have been disabled.

As well as reducing the attack surface that a malicious actor might manipulate – thus significantly reducing risk – adopting this 'regular clear-out' principle also removes the requirement for upgrading and updating unnecessarily. Efficiency and productivity will be improved significantly as you cut your patching to-do list down to include only the updates you actually need. The UK's National Cyber Security Centre include this crucial tip in the Secure Configuration element of their ['10 Steps to Cyber Security'](#).

While personal data should have been a regular feature on the 'Use It or Lose It' list, until recently, it has not been. The recent changes in data protection legislation around the world are providing a rather heavy financial incentive to take it seriously from now on.

However, even disregarding the potential fines (which are only imposed after the event in any case), deleting unnecessarily held personal data can potentially reduce the need for any engagement with data protection regulators. One of the critical considerations involved in reporting to regulators is the number of records affected. Retaining only the personal data that you actually require to run your business will help to keep that number down should an incident occur.

The 'use it or lose it' principle has been around for a while and it is being applied by some cyber security and privacy professionals, but there is still much more that can be done.

- Survey your cyber estate to identify software, hardware or services you no longer require. Include the view from the outside in, and run a host discovery and passive risk assessment. Whenever we undertake this for clients, we invariably uncover a number of surprises.
- Apply this 'use it or lose it' principle to your identity and access management as well. While contractors and temporary staff may only be working with your organisation briefly, virtually they can remain there for ever if you are not tidying up properly as you go.
- Review the personal data that your business needs to function and

provide products or services to clients and customers. Delete any data that you no longer have a business need to process. Of course, make sure that you apply your retention policy before you do.

The ever-changing world of cyber security and privacy threats makes it difficult to reduce risks to an acceptable level and then manage them. However, we have found that most organisations could improve their situation and diminish potential risks significantly by taking just these few simple steps.

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

### Contacts



#### **Press Office - Group and UK**

Press Contact

[nccgroup@thisismc2.com](mailto:nccgroup@thisismc2.com)

+44 (0)161 236 1352



**Al Loehnis**

Press Contact

Maitland AMO

Financial Results Media Enquiries

+44 (0)20 7379 5151



**Press Office - North America**

Press Contact

[NCCGroup@cdc.agency](mailto:NCCGroup@cdc.agency)

+1 408 776 1400

+1 408 893 8750