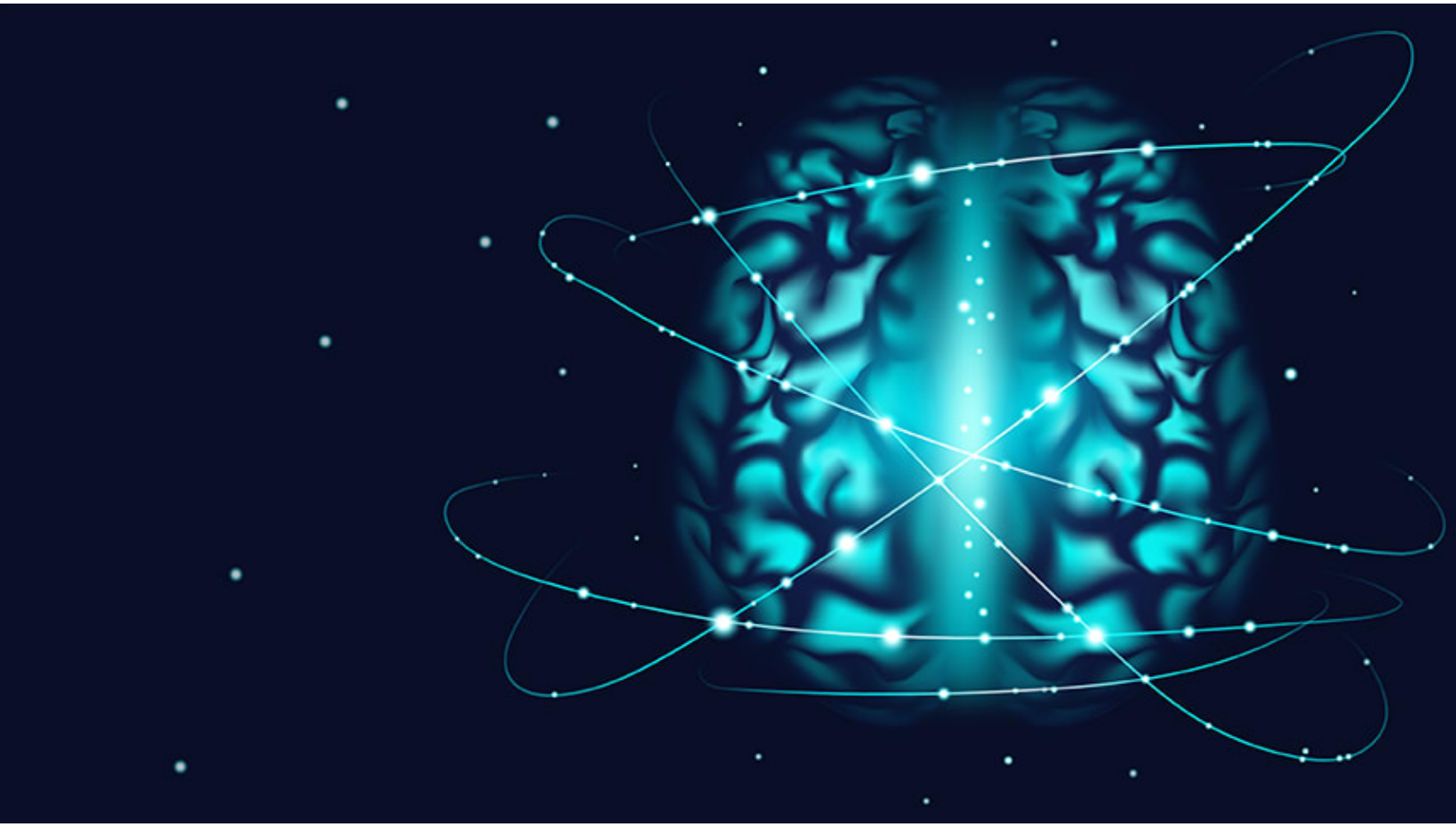

Apr 04, 2019 23:16 BST

Cyber security is evolving into a science

Cyber security is still a relatively young industry. However, in the book Superforecasting: The art and science of prediction, there is an interesting analogy, which can be drawn between medicine in the 1800s and the majority of modern day cyber security advice.

The 1900s saw the advent of double blind trials and various other means for measuring the efficacy of different treatments. This has allowed us to understand what really works and what does not in medicine. Before this, there was a lot of conflicting advice being given and drugs being administered without truly understanding the outcomes.

Similarly to 1800s medical practices, with the advice given or claims made by

cyber security vendors at this point, it can be difficult to truly understand what will improve the situation, by how much, for how long, and with what dependencies or constraints.

Approaching the issue scientifically

In 2014, I saw a presentation aimed at cyber security professionals delivered by Cormac Herley of Microsoft Research, titled Learning to Self-correct: Approaching the questions of harm and security scientifically.

The presentation was powerful and thought-provoking. Cormac encouraged the audience to avoid contradictions in their marketing material, and to stop treating slogans such as “there is a tradeoff between usability and security” and “no security through obscurity” like Newton’s Laws.

He also reiterated the fact that there are no exemptions from burden of proof, and urged security professionals to stop invoking security exceptionalism. We are after all not immune from making mistakes the way others do, such as sloppy thinking, confirmation bias, vague claims, jumping to conclusion.

Looking at these points we can see much of what the security industry is good at – namely, being a snowflake and coming up with slogans, which are then repeatedly cited as laws.

While academia is playing an increasing role in cyber security research, we still have much to do when it comes to the measurement of effects in real-world environments, systems and ways of working.

Opinions and industry best practice challenged by science

In the same presentation, Cormac also presented that "definitions don't describe the world", with the concrete example of "To be secure a password must be of length eight and have three of the four character classes (lowercase, uppercase, digits, special characters)."

Now, in isolation, this statement seems logical and has its roots in a NIST publication from 2003 and Special Publication 800-63. Then you impose a rotation schedule and you quickly realise that people cannot remember all

their passwords without a password manager, and so default to a pattern or system together with various other poor hygiene behaviours.

Fast forward to 2016, when the UK's National Cyber Security Centre's SocioTechnical team released its new password guidance. This publication contradicted a lot of the previous industry best practice and risk professional advice. Instead, it was based on research conducted at University College London starting in 2010 in a paper titled The True Cost of Unusable Password Policies: Password Use in the Wild - or dare I say it 'science'.

This research showed what happened when you put unrealistic expectations on users with such policies in the real-world.

The world is changing

We have recently seen the emergence of MITRE ATT&CK and its use in the measurement of end-point detection coverage against real-world actor tradecraft.

Real-time simulations of an attack are now available, and can provide insights including the independent and quantifiable measurement of Security Operation Center detection rates and speeds. Meanwhile, rebuilt variants of common ransomware, such as EternalGlue, allow the real-world measurement of the efficacy of the architect, controls and operations designed to minimise the impact of a NotPetya style worm.

These types of solutions enable organisations to cut through marketing claims and assertions, and understand what really works in the real world based on evidence through processes that are repeatable.

My prediction, based on seeing where government policy, academia and mature businesses are converging is the industry is about to accelerate in its application of such rigor.

Why? Firstly, budgets are big and mature organisations want to better understand their return on investment.

Similarly, the market is awash with solutions from vendors and service providers. It is increasingly impossible to understand which solutions actually

move the dial and which do not in terms of cyber resilience, by how much, for how long and against which risks.

This complexity coupled with the regulatory environment means that governments, organisations, boards and leadership want to know what they are doing actually works against the risks they deem unacceptable – as alongside, increasingly, their insurers.

What's next for the cyber security industry?

Simply put, all providers bear a responsibility to their customers. It's important to understand if the remediation advice given has been shown to actually improve the situation, or if it's only anecdotal.

The sector will continue to devise new methods of measurement - from risk management strategies through to technical counter measures. These measurement techniques will be applied to understand the things that actually materially improve the situation for customers depending on their budgets and maturity.

The shift to a more scientific, analytical industry is unstoppable and necessary. It will result in better quality advice and outcomes for customers, which will more efficiently and effectively allow them to manage risk. This will help make the world safer and more secure.

Image credit: Shutterstock image ID: 1260477022

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 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750