KASPERSKY lab

IT ain't what you do (it's the way that you do it)

Why AI and behavioural biometrics, on their own, are not the answer to all your cybersecurity woes

By Neira Jones

More than 20 years in financial services and technology made Neira believe in change through innovation and partnerships. She is regularly invited to advise organisations of all sizes on payments, fintech, regtech, cybercrime, information security, regulations (e.g. PSD2, GDPR, AML) and digital innovation.

She always strives to demystify the hype surrounding current issues and also enjoys her work as an expert witness for matters related to payments security. She likes engaging on social media and regularly addresses global audiences as a keynote speaker or chair-person, as well as being a regular press commentator.

She is a Non-Executive Director for Nasdaq-listed cyber security firm Cyber1 and also chairs the Advisory Board for mobile innovator Ensygnia. She is a partner for the international Global Cyber Alliance and ambassador for the Emerging Payments Association.

She appears on the Planet Compliance Top 50 RegTech Influencers, the Thomsons Reuters UK's top 30 social influencers in risk, compliance and regtech #TRRiskUK30 2017, the Jax Finance Top 20 Social Influencers in Fintech 2017, and the Innotribe Femtech Leaders List, amongst others.

Tripwire nominated her "Top Influencer in Security to Follow on Twitter" in January 2015, CEOWorld Magazine nominated her Top Chief Security Officer to Follow on Twitter in April 2014, she is the Merchant Payments Ecosystem Acquiring Personality of the Year 2013, the SC Magazine Information Security Person of the Year 2012 and has been an InfoSecurity Europe Hall of Fame alumni since 2011, as well as being voted to the Top 10 Most Influential People in Information Security by SC Magazine & ISC2 in 2010.

She has previously served on the PCI SSC Board of Advisors for four years, is a Fellow of the British Computer Society and has worked for Barclaycard, Santander, Abbey National, Oracle Corp. and Unisys.

Her clients include financial services institutions, FinTech companies, consulting organisations as well as information security and technology providers.

@neirajones

Isn't it funny how **biometrics**, a science that has been around for centuries[1], did not enter the public consciousness until Apple launched Touch ID with the iPhone 5S in September 2013? As a result of both government and consumer pressure, **biometrics** adoption has been staggering, and the global market size is now predicted to reach $59.31 billion by 2025, with a CAGR of 19.5% during the forecast period[2].

Of course, this technology, like any other, whilst offering tremendous potential, is not the be-all and end-all of **fraud** and **cybercrime** prevention[3]. In one incident, for example, a Nest doorbell owner was mistaken for an intruder because he was wearing a Batman T-shirt. This perhaps goes some way to proving that technology, when taken in isolation, is not always capable of protecting an organization or individual from criminals who constantly evolve at the incredible pace of the **digital** age.

Consumer pressure and regulations have been the main drivers. On one hand, consumers want more ubiquity, speed and safety. Indeed, consumers are experiencing both password fatigue and data breach lassitude. On the other hand, regulations aim to protect consumers and ecosystems, whilst fostering innovation and competition.

As organisations increasingly strive to simplify the user experience and remove friction from interactions, some have turned to **behavioural biometrics** to try and deploy dynamic means of authenticating genuine users (e.g. the way you walk, type or even hold your phone), in an attempt also to satisfy regulatory pressure.

The key to successful deployment will come down to one thing: context. Indeed, long gone are the days where role-based **authentication** measures were sufficient to manage **risk**. In fact, as far back as 2014, Gartner predicted that by 2020, role-based **authentication** controls (RBAC) would be superseded by mechanisms relying on knowledge of attributes (ABAC) and contextual information to make decisions[4]. Whilst we have seen some successful deployments of such methods, they are not yet the preferred choice.

This is perhaps due to the fact that software development methodologies are still slow to incorporate ABAC, or that there are not yet enough vendors providing **identity** and attributes services; this could also be due to a lack of interoperability of the various deployments, or indeed – whilst competition generates pressure to innovate and become more **digital** – to the fact that legacy applications are slow to migrate and that policy and rules are difficult to develop; or indeed because of the increased focus on **data protection** and **data privacy**.

Indeed, this last driver is the main reason for the change in consumers' perception of breached organisations[5] in recent years, where over half (57%) now blame companies rather than criminals if their data is stolen or mishandled. This consumer backlash, in response to numerous high-profile data breaches and conducive regulations putting consumers in a position of power, has exposed one of the hidden risks of **digital** transformation: the loss of customer **trust**.

Biometric verification. Facial recognition based on a polygonal grid created by connecting points on a face.

In our fast moving **digital** world, regulators are trying to address the multi-faceted challenge of protecting consumers, whilst fostering innovation and economic development. The ever-increasing amounts of data flowing across ever-blurring geographical boundaries make it increasingly difficult to catch up with criminals and develop regulations able to cope with new technologies and new crimes.

The business conundrum is therefore to ensure customers are genuine (with secure **authentication**) and to prevent **fraud**, whilst collecting more data to deliver exciting and seamless experiences, all the while maintaining consumer **trust** and **privacy**. And to that effect, if we examine some of these regulations more closely, it will become apparent that many requirements overlap. For example, stringent customer **authentication** and **fraud** prevention measures are required by PSD2[6] (Strong Customer **Authentication**; Transaction **Risk** Analysis), the various Anti-Money Laundering regulations/directives (**KYC**[7], **eKYC**, due diligence), the GDPR[8] (protection of personal data and sensitive personal data), to name but a few.

Similarly, requirements for incident response and timely disclosure of security incidents is required by, amongst others, the PSD2, the GDPR, AML regulations/directives and the NIS Directive[9]. And last but not least, the requirements for data and **information security**, privacy and protection are common to all of these and many more...

And whilst the regulators grapple with their long regulatory cycles and try to make regulations future proof, the world moves on. And consumers adopt more and more technologies, and share more and more data, and demand safety. In the meantime, **mobile** device ownership has overtaken personal computers[10], with smartphones now established as the preferred mode of consumer interaction and social media as the third shopping channel[11].

And consumer technology adoption doesn't confine itself to **mobile** devices: the Internet of Things (**IoT**) has now infiltrated our lives. Whether it is Alexa, a Nest security camera, a fitness monitor, a smart watch or a connected toy[12], these technologies have endeared themselves to us with their simplicity and convenience, often at the expense of security and safety.

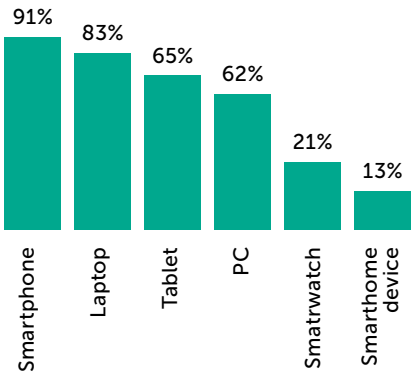
As the socio-economic landscape evolves, with the emergence of the gig-economy, the increase in remote and **mobile** working, the adoption of "everything-as-a-service" and cloud computing, the concept of "**identity** management" now has to include what people own, share, and use. "Things" are becoming part of our lives and must therefore be identified and managed accordingly. "Things" are now part of the "Context" in which we interact, and as enterprises increasingly adopt intelligent devices and other endpoints (such as BYOD[13], electronic tags, sensors, process and distributed control), the attack surface grows accordingly.

The lack of interoperability and standards, combined with the disparity among industries and jurisdictions, only serves to increase complexity. And whilst a focus on technology is legitimate, we must not lose sight of the human element: social engineering is still the dominant cause of data breaches, which reminds us of the fact that a good **cybersecurity** strategy should always include the three elements of "People, Process, and Technology".

---

1 The History of Fingerprints
http://onin.com/fp/fphistory.html
2 Biometrics Technology Market Size
https://www.grandviewresearch.com/press-release/global-biometrics-technology-market
3 Man mistaken for Batman by his Nest doorbell
https://www.shropshirestar.com/news/viral-news/2018/09/18/this-man-was-locked-out-of-home-when-his-smart-doorbell-thought-he-was-batman/
4 Gartner Predicts 2014: Identity and Access Management
https://www.gartner.com/doc/2630035/predicts--identity-access-management
5 The Dark Side of Customer Data, RSA
https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data
6 The 2nd Payment Services Directive
7 Know Your Customer
8 The General Data Protection Regulation
9 The Directive on Security of Network & Information Systems
10 © Experian Global Fraud & Identity Report 2018
11 © Bazzaarvoice Shopper Experience Index 2018
12 **https://www.theregister.co.uk/2019/02/08/privacy_fail_kids_smartwatchmaker_hits_back_at_bad_pr/**
13 Bring Your Own Device

Device ownership



Undoubtedly, our current landscape not only presents an ever-growing attack surface, but also a complex regulatory maze. This complexity has generated the need for more and more **automation**, which itself has engendered an increased focus on technologies which deliver such **automation** (e.g. **AI**, **machine learning**, behavioral analytics), and the birth of a new buzzword: RegTech, **meaning Regulatory Technology, or the application of technology to enhance regulatory processes**.

But let's not be fooled: whilst **automation** has become a necessary component of any **cybersecurity** strategy, it alone does not make a sensible or even viable strategy. Of course, in an ideal world, technology would be able to spot and stop crime without human intervention. Unfortunately, one thing gets in the way: Real Life.

Technology is only ever as good as its designers, and the data available to derive insights is neither perfect nor completely accurate. Furthermore, technology can also be used against itself, as evidenced by the emergence of methods such as "Adversarial **Machine Learning**" where malicious attacks can be designed to subvert defensive technologies in order to appear legitimate or inoffensive.

So let's not get swept up by the hype, any technology solution claiming absolute protection should be treated with caution. Whilst technologies such as **AI** or behavioral **biometrics** have a legitimate place where a specific **risk** can be mitigated by their use, a good **cybersecurity** strategy will always come down to common sense: **any technology, on its own, will not do the job**.

As always, the basics will need to be covered first, and the risks specific to the organization will need to be managed, just like any other **risk**. Technologies will need to be deployed, and they will not necessarily be sexy (e.g. endpoint protection, malware detection, access management, etc.). And the appropriate processes will need to be put in place to make those technologies effective (e.g. incident response, software life-cycle management, supply chain governance, patching, encryption, etc.).

And of course the human element will need to be addressed, both internally and at the consumer level (e.g. training, education, end-user policies, acceptable use, etc.). Deploying a layered approach, where **automation** is used and where the processes lend themselves to it, will free staff to concentrate on complex cases or reviews and value-adding activities. Again, everything has its place, in the right context.

Kaspersky®
Fraud Prevention

You can get more information about products and services from Kaspersky Lab partners or from the website: www.kaspersky.com.

Kaspersky Lab HQ Office
39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation
info@kaspersky.com
www.kaspersky.com