HUMAN BEHAVIOUR AND DIGITAL TRUST:
HOW UNEXPECTED REWARDS CAN IMPROVE CYBERSECURITY, PROTECT CRITICAL INFRASTRUCTURE AND REDUCE COSTS

By Chris A. Jones, George Runger and Jack Caravelli

"Most cybersecurity problems are caused by people being careless with their own information."

- Former US Secretary of State Condoleezza Rice (30 January 2017)

Technology has always been an amplifier of human values and emotions. The increasingly accelerated advancement of technology is putting our values and vulnerabilities as a society into sharp relief. For this reason, thinking about trust across all forms of digital access and activity levels (see: Internet of Things) has become imperative. It is essential to optimize human-machine trust so that it aligns with our humanity, ethics and fair social contracts. The challenge is that traditional risk management strategies often do not translate well to present-day distributed and dynamic networks; indeed, they have struggled to keep up with the increasing sophistication of cybercrime.

Such cybercrime is most often publicized when enterprises or individuals are financially exploited. However, these crimes are widening in scope to inflict damage that is both social (exploiting a person's "likes" and "followers") and physical (compromising power grids, cars, homes or even medical devices) in nature. A particularly important sector for concern is the $4 trillion global healthcare economy. Health records are vulnerable across the healthcare continuum, including imaging, supply chains, care delivery, hospitals and pharmaceutical databases, as well as the corresponding billing required to pay for these goods and services.

Even more worrisome is that now, for the first time ever in the history of humanity, the human body itself

is now subject to cyber-attacks (see: Future Crimes by Marc Goodman on the hacking of medical devices, ch. 14, "Hacking You"). A recent white hat hacking demonstration showed how easy it is to hack a bionic prosthetic limb with the intent of causing malicious harm. When one loses control of their body, it not only increases the cost of doing business, for example, through the administration or insurance of additional healthcare; it is a violation of personhood and the societal values we hold dear.

Health (our bodies) and finance (property) are the bedrocks of our social contracts. The notion that cyber security is only as good as its weakest link begs the question of what we can do to fortify ourselves against our vulnerability to cyber-attacks.

How do we solve this problem? Improving the security of centralized information, servers and cloud encryption, as well as improving human behaviours, would be a good start. Humans are often "in-the-loop" and as such are affected by the outcomes of such attacks, but cyberattacks operate outside of the traditional rule and trust structures of many societies. Whereas computers can be unplugged, human beliefs are much harder to change and require a dynamic, multi-faceted approach. Incentivization to do the right thing (see www.trustr.us) by motivating, educating and rewarding end user behaviour, such as through improved "cyber-hygiene", will address some of the weakest links. Better levels of encryption (see www.ensurity.co), combined with secure communications such as closed user group communications (see www.cqr.global) that create the equivalent of a virtual private network, will address other vulnerabilities. Moving computer activity to a distributed computing environment known as the Blockchain will further protect the sanctity of the human-digital dyad, but only if it is truly decentralized. The widely popular crypto-currency called Bitcoin is not truly decentralized, because the majority of the value creation and manipulation capabilities lie in the hands of a few Bitcoin miners.

A welcome trend for sensitive areas such as healthcare and finance is the shift of computing towards a more distributed ledger technology, meaning that not only will future computing be truly distributed (like Napster), but also that it will have an inbuilt immutable ledger (see distributed ledger technology or DLT). Security will be achieved when individual transactions are grouped into "blocks", which are "hashed" like a fingerprint; each block thus becomes inextricably linked or "chained" to the previous one.

Newer platforms are developing new ways to still be secure without having to group transactions into blocks and without having to link up these blocks in a chain. The upside of all of this is that it will solve the scale problem of mass adoption. If blocks and public key infrastructures (PKIs) are too heavy, too energy intensive, too slow, not quantum-secured and vulnerable to "blockchain hoarding" or manipulation, then critical infrastructures will not be able to reap the benefits of the blockchain. On existing blockchains, when the send of a transaction pushes a transaction to the recipient, all of the verifying entities can "see" the plain text data in the middle "nodes". The visibility of the transactions thus opens them up to cyber abuse, whether this be from front-running, insider trading or other abuses concerning inappropriate access to confidential information.

At the heart of the blockchain ethos, the consensus method validates a transaction when there is no trusted mediatory third party; instead, a stranger validates transactions between two parties and a "consensus"

is reached as to the validity of the exchanged information. The consensus method has its problems, however. Take the example of somebody buying a home, who should only need to show proof of income and their credit rating, as opposed to their entire life history including unneeded personal information such as race, class, education, sexual orientation and marital status. Another example might be hospital patients, for whom there should be different levels of access – only information that is required to make a medical decision ought to be displayed, rather than personal aspects such as social security number, postcode, income or insurance status. Such "zero-knowledge proof" or "selected obfuscation" is one of the great opportunities to be provided by blockchain technologies. These challenges are pragmatically complex and, because the complexity cannot be easily reduced to simple analogies and because there are still many questions surrounding digital security, blockchain has tended to only be applicable to the solution of esoteric challenges. Indeed, because blockchain developers do not usually come from a cybersecurity background, the cryptography aspects of blockchain technologies have tended to be an afterthought, rather than embedded into their design from day one. This dilemma highlights certain educational challenges, whereby even similar verticals may not fully engage with one another's expertise. Therefore, collaboration is becoming essential in the digital era.

One of the most recent collaborations in this respect is a project called TrueNet, which combines cyber security and blockchain to solve three key challenges, namely: ensuring privacy and confidentiality for all parties, safely securing the encryption of plain text data and only keeping a hashed image of every encrypted transaction. This so-called zero knowledge secret sharing (ZKSS), which proves individual transactions within a timeframe of milliseconds, will make blockchain technologies much more attractive to critical infrastructures. Using this method, it is envisaged that the most salient of problems faced by the healthcare, energy and finance industries on a daily basis, whether these be time-, cost- or security-sensitivity, will be solved using this more secure form of distributed ledger technology.

DEFINING DIGITAL TRUST – IT'S ALL ABOUT BEHAVIOUR

Trust is a very human quality and, like other human traits, it is subject to cultural and societal variation. Stated simply, trust is belief in the ability, reliability, truth and integrity of someone or something. Trust usually means accepting that someone or something is true in terms of how they work or function, as well as how they behave towards others. Trust can take many forms. People have complex behavioural motivations and tendencies. Some people may want to write down their passwords next to their computer so as to easily remember them, while other people spend their lives hacking into critical infrastructures for the purpose of creating unrest. Human trust takes time, often years, to build, and even more time to regain once breached. Digital trust, on the other hand, is tested within a timeframe of nanoseconds, and is routinely breached, righted and quantified, so as to maintain a level of confidence between humans, computers and the networks between them.

Digital trust refers to the connections between people, data and networks. In the cyber world, this form of trust is built by the continual verification of the integrity of people, access points and connected systems. People rely on usernames, passwords and other levels of authentication to establish an identity, which allows them to gain access to machines, applications and devices. Similarly, machines authenticate using digital keys, caches and certificates for secure machine-to-machine communications, as well as to establish machine identity security.

In the modern era, there are at least three actors on any network: trusted people, untrusted people or untrusted bots, and the machines or connections that enable these communications. Digital trust is the foundation of every digital touch point between people and devices. Digital trust is grounded in the expectation that an actor or group is/are precisely who, or what, they claim to be.

ASSESSING RISK FROM THE MCKINSEY REPORT[1]

Given the radical transformation of network infrastructures, every organization, regardless of the size or industry, needs to regularly examine its exposure to cyber risks and prepare for a potential incident. The basic formula is Risk = Threat x Vulnerability x Consequence. While this may seem simple on the surface, getting the depth or information required to make a risk calculation is not trivial. Historically, organizations have focused primarily on reducing and managing the threat and vulnerability components of that equation. We need to understand the kinds of devices that are operating on our networks: where are vital operational data located, who has access to these resources, and how do applications and services connect these things together? Managing such elements of the equation has become increasingly complicated due to the volume and increased frequency and intensity of security breaches. It can be argued that, demonstrably, our cybersecurity of critical infrastructures has not been particularly effective. Part of the problem is that the isolated and often disparate security tools and platforms currently deployed in our networks for addressing threat and vulnerability were never designed to protect today's complex ecosystems, particularly human vulnerabilities and digital trust resources. Consequently, they rarely contribute to an organization's crypto agility.

Crypto agility (or cryptographic agility) is the capacity of an enterprise's IT system to easily evolve under dynamic management and to adopt alternatives to the cryptographic principles it was originally designed to use, as digital trust itself evolves. As we move infrastructure and services to the cloud, implement and adopt IoT technologies, embrace a more mobile workforce and acknowledge the growth of shadow IT (according to which data and services live outside the network, and therefore are often out of the sight or control of the IT organization), the potential attack surface and risk grows exponentially. Comprehensive digital trust is therefore essential.

In order to increase the effectiveness of digital trust risk management, resources must be concentrated on consequences. Defenders must invest time and energy in understanding the kind of data that is worth protecting, who and what can access it and how to manage the associated risk.

As there are typically hundreds of thousands of keys and certificates present in enterprise environments, the challenge and complexity of this problem is enormous. Manual management processes that only rely on individuals and personal experience cannot deliver an effectively integrated and dynamic digital trust risk management system.

CONCLUSIONS

There are still many questions surrounding the democratization of access to blockchain and cybersecurity in the case of a power, digital or digital-speed divide. Reflecting on just the past few months, the ever increasing hyper-connectivity of devices and networks, the exposure of software and firmware to vulnerabilities, the globalization of the digital economy, advances in cybercrime techniques including the manipulation of democratic votes using social media and methods of funding them, using cryptocurrencies, as well as the commercialization of "crime-as-a-

1 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/a-framework-for-improving-cybersecurity-discussions-within-organizations

service", have all resulted in an explosion in the frequency and severity of cyberattacks.

It is our firm belief that, once next-level blockchain technologies have been proven and widely adopted, gaining an understanding of the psychological motivation for cybersecurity will be able to reinforce trust in the human-digital dyad. Moreover, a proverbial "pat on the back" or even a relevant reward from a colleague or even a chatbot, when used to reinforce a sense of personal responsibility for safeguarding data, cyber access and good cyber hygiene, may be the most effective, cost-efficient and underutilized resource we have to build and maintain digital trust over the long term horizon.

Moreover, this may potentially still be insufficient, as robust workflows are needed to embed digital trust at the heart of operations. Human-in-the-loop security processes need to become as critical as it would be to administer the correct drug to a patient. The human element of security is what the organization does every day, in a variety of ways. It is reinforced, measured, reported, reviewed and improved as is done for other critical business processes. The approach that was previously applied to behaviour is now considered to be insufficient for the next cycle; just as threats are evolving, an increased focus on behaviour is also continuing over time. Here, the digital technology that is under threat could potentially assist with increasing security. Immersing ourselves in a space surrounded by recommended practices (digital notes, chatbots, digital rewards, etc.) reinforces the desired behaviour.

We know from Nobel Laureate Richard Thaler that our beliefs are not always rational and there are many ways in which to nudge improvements in human behavior. We know from behavioural experts like Stanford professor Robert Sapolsky that the anticipation of a reward is more salient than the reward itself. Why these insights have only begun to enter the sphere of cybersecurity is alarming. The human element of security is what any solvent organization does every day, in a variety of ways. Human behaviours are reinforced, measured, reported, reviewed and improved as is performed across other critical business processes. The rule-based playbook of cyber security has become antiquated, however, as human motivations are not easily reduced to a single unit of value. We are faced with rules that are considered to be insufficient for the next cycle: just as threats are evolving, human behavioural complexity is growing and becoming more nuanced, even more malicious, over time. The good news: our very digital technologies that are under threat could potentially assist with increased security. Health and financial information could be used as a digital fingerprint, once its integrity is safeguarded from misuse. We have only started to learn the benefits and risks surrounding quantum computing and blockchain, but applying these technologies to map our understanding of the human experience better will go a long way towards protecting our society and critical infrastructures. There will be mistakes along the way, and countries may prefer to be fast-followers rather than pioneers. As a first step, to maintain the values that we as a society hold dear, we must improve our cyber hygiene. We can then embrace time-saving technologies (sensors, chatbots, digital rewards, etc.) that can be quickly iterated towards improved value at very marginal costs. ■

AUTHORS' NOTES

- According to Gartner, 87% of CISOs are "… unaware of the scope or status of their X.509 keys and certificate deployments until it's too late".
- Downtime and system failures are often caused by certificate expiry and key errors. Increasingly, compromised assets such as these are leading to significant data breaches.
- Digital keys and certificates are a primary target for exploitation by cyber hackers and malicious insiders. More than 55% of current attacks exploit these vulnerabilities.
- A lack of trust in the identities of the machines that control the flow of mission critical data is a source of significant risk which, if unaddressed, leaves organizations vulnerable to serious breaches.
- Invalid, inactive, stolen or compromised digital credentials are a major security threat to enterprises.

- The EU GDPR requires that enterprises have robust, transparent and compliant processes in place to prevent the above scenarios from occurring. The GDPR imposes significant fines in the event of a single breach, being €20 million or 4% of the organization's annual worldwide turnover, whichever is greatest.

ABOUT THE AUTHORS

Dr Chris Jones is director of venture investments for Vermont's largest hospital network. He is also associate professor of behavioral economics at Arizona State University, voted #1 in innovation by U.S. News and World Report.

A serial entrepreneur, Jones invented the award-winning chatbotting tool called trUStr.us. He is leading strategic healthcare projects for a blockchain start-up called TrueNet and was a keynote speaker at the 2018 world meeting of the International Society for Pharmacoeconomics and Outcomes Research (ISPOR). He is an elected member of the New England Comparative Effectiveness Public Advisory Council of the Institute for Clinical and Economic Review (ICER), and a fellow of both the Royal College of Medicine and the European Centre on International Political Economy (ECIPE).

Jones holds a bachelor's degree from the University of Michigan, Ann Arbor, and master's and doctoral degrees from the University of Oxford.

George Runger PhD is Chair of the Department of Biomedical Informatics (BMI) at the International School of Biomedical Diagnostics, a Professor in the School of Computing, Informatics and Decision Systems Engineering at Arizona State University and an Adjunct Professor of Biomedical Informatics at Mayo Clinic. He is also Director of the Center for Health Information and Research (CHIR) at ASU. CHIR collects health information from a variety of sources across the state and uses the information for multiple health improvement projects. He researches analytical methods for knowledge generation and data-driven improvements in systems with a focus on large, complex data and applications in monitoring, surveillance, decision support and population health. Previously, he was a technical leader for system improvements and analytics projects at IBM. He has published over 100 journal articles in the field of analytical methods in journals such as Machine Learning Research, IEEE Transactions and Pattern Recognition, and has been funded by national agencies as well as corporations (e.g., current projects include cognitive computing with Intel and safety with Federal Express). He was selected as the inaugural department editor for healthcare informatics for IIE Transactions on Healthcare Systems Engineering.

Dr Jack Caravelli is the author of the recently published book, "The Age of Hatred: ISIS, Iran and the New Middle East", which is listed on both the UK and US Amazon websites. His service career in the US government included a senior assignment on the staff of the White House National Security Council, where he was President Bill Clinton's principal adviser on Russian and Middle Eastern non-proliferation issues. Mr Caravelli also served as a senior official at the US Department of Energy, where he managed the Department's threat reduction programmes, which worked to secure nuclear and radioactive materials at risk of theft or diversion in Russia and other parts of the former Soviet Union. He has also authored other books on national security policy, has appeared on the BBC and is a regular guest on various US television and radio talk shows. He is a visiting professor at the UK Defence Academy.