Baker McKenzie.

Commentary

August 2025

International: What road safety can teach us about cybersecurity

Contents

In more detail

Bibliography

In brief

Cybercriminals are fond of entities with a particular asymmetry: assets and data in abundance and defenses in deficit. In recent years, security attacks have become increasingly advanced, and commercial entities have achieved fair proficiency in defending their information in the cyberspace. However, private non-commercial entities with the same resources have not taken nearly the same precautions, resulting in underdeveloped cybersecurity protocols compared to the wealth they manage. Therefore, family offices and high-net-worth individuals (HNWIs) have become very attractive targets.

This article appears in the second edition of the Private Wealth Newsletter 2025.

In more detail

A significant aspect of this discrepancy concerns policy: large companies uphold cybersecurity regulations because they are mandatory. Governments understand that it is in their best interest to impose these regulations, not only because large sums of money flow out of the country when cyberattacks are regularly successful, but also because in times of geopolitical unrest, adversaries will often target critical infrastructure to undermine societies. One such protective measure is the 23 NYCRR Part 500 cybersecurity regulation, which was amended by the New York Department of Financial Services to require New York insurance companies, banks and other financial service institutions to adhere to several cybersecurity criteria. Among other things, these companies are required to conduct regular penetration testing and vulnerability assessments, implement technical and organizational security measures like encryption, MFA and limited access privileges, and they are required to give a 72-hour notice if a cybersecurity incident occurs. (BakerWorld, accessed 2025) In addition to financial services, similar rules are in place for companies that perform critical services, such as companies that operate chemical facilities, sustain wire or radio communications, or provide essential public health services.

Alternatively, family offices and HNWIs operate with less direct oversight and are not subject to the same regulations. The extent to which they protect their devices and accounts is a personal decision, which makes it susceptible to various oversights. For one, family offices hesitate to invest in security until they experience an incident firsthand. This results in 31% of offices not having a cyber incident response plan in place. (Deloitte, 2024) Moreover, cybersecurity protocols that are implemented often do not form one integrated system. These families will have multiple homes with different online security systems for each one, multiple cameras, devices and networks. A particularly lethal cyberattack can take place when the attacker incrementally gathers personal information, without being detected, and waits until a large transaction is due. Therefore, these isolated security features are especially dangerous because if one of these devices is attacked, the others will remain unaware and vulnerable. These weaknesses are transparently known. Deloitte's 2025 Family Office Security Report found that over the last 12 to 24 months, 43% of family offices globally experienced a cyberattack. Among the family offices which experienced a cyberattack, one-third suffered some form of loss or damage as a result. (Deloitte, 2024) These attacks threatened personal wealth, posed disruptions to data security and sowed social mistrust.

However, we cannot ignore the second non-digital side to these breaches. Granted, impaired cybersecurity allows hackers to accumulate the necessary information to deliver a personalized attack, but the decisive factor which makes the attack successful depends on human gullibility. Phishing — contacting someone via fraudulent email or message — makes up 93% of cybersecurity threats, and these messages exploit various human vulnerabilities to push for a financial transaction. (Deloitte, 2024) We know that the most consequential cases of phishing arise when overconfidence is paired with other inhibition-lowering emotions, for example, excitement. Luxury items and collectibles are often very expensive, but also very exciting purchases. The excitement around these purchases can be so great that one ignores things about the purchase that don't seem right. There seems to be a positive correlation between positive emotions and perceived security in judgments involving risk.

A study conducted by Lerner & Keltner in 2001 observed how happy participants expressed optimistic risk estimates, whereas fearful participants expressed risk-averse estimates. (Lerner and Keltner, 2001) In a similar 2007 study, Plassman, O'Doherty and Rangel found that financial risk is more likely to be endured when the product has the potential for pleasure. (Plassmann et al., 2007) In this study, MRI scans showed increased activity in reward centers — and decreased activity in risk-assessment centers — when subjects experienced positive emotions relating to the products that they were considering buying. At the 2025 Bloomberg Family Office summit, Crypto.com chief information security officer Jason Lau insisted that overconfidence was the single biggest cybersecurity threat for family offices. He assured the audience in a pithy aside: "Hackers — they don't really care about how smart you are — all they really care about is how unprepared you are." (Bloomberg Family Office Summit, 2025)

Any weakness in judgment, no matter how small, can be decisive, because hackers play the long game. Hackers will gather whatever information they can, and they will wait until a large purchase is made — a period of time known as the dwell time — so any kind of data leak, any number of years ago is significant. Knowing when and what kind of transaction is being made, they can swoop in with all the right information at the critical moment. The 2020 boom in e-commerce made this swooping very easy, since moving large sums of money online became commonplace. The fastest growing market in e-commerce fraud is collectibles, which experienced a 106% surge in 2024, closely followed by the 104% surge in luxury goods. (CropInk, 2025) These are not surprising epicenters of e-commerce fraud. Luxury goods are especially lucrative targets, and their online presence is growing quickly. About two-fifths of the global luxury goods market is currently generated via online channels, (Statista, 2025) and the DHL report predicts luxury e-commerce sales to reach USD 65 billion by 2025. (DHL Customer Solutions & Innovation, 2024)

Our challenge is delicate: we want cybersecurity systems to be seamlessly operable by citizens, but sternly resistant to their cognitive weaknesses. Thankfully, this is not the first time we have tried to converge human impulses, assumptions and biases with a technological or mechanical interface. A common example is managing traffic in urban areas. Let us briefly assume that both the human and machine fronts of the equation are perfectly optimized. On the human front, our drivers are physically sound — having stellar vision, good reflexes, showing no propensity for seizures or any other uncontrollable bursts of movement — and they are mentally sound — able to exert reasonable judgment on various situations, and not under the influence of drugs or alcohol. On the mechanical front, our car components, like the brakes, wheels and engine, are all sound and responsive. Two interesting questions ensue. How do we combine these two robust systems of human and machine intelligence to form one capable unit? And how do we move this unit quickly and safely from location A to B?

We can liken this integration problem to human users and digital security. How do we model user interface so that a person and their device forms one capable unit? This has been paid enough attention since Donald Norman coined the term user experience design in the early 1990s. More interestingly, assuming that the HNWI is optimally informed and that their accounts are optimally armed against cyberattacks, how do we design the cyberspace so that this unit can perform transactions, share information and communicate with other such units, in a fast and safe manner? Our most persistent cybersecurity gaps cannot be addressed by simply improving data protection code or telling people to be more careful.

The digital face of cybersecurity is already a robust dance. Cryptographers are constantly devising new ways to safely encrypt and decrypt information, and these algorithms are consistently getting bypassed by hackers.

© 2025 Baker & McKenzie | 2

As technology progresses, both parties are in the business of outpacing each other. Additionally, we need to rid ourselves of the illusion that maximally warning people about the presence of hackers will proof the cyberspace the way we hope it might. No amount of repetition will correct the years of evolutionary biology that led us to make decisions the way we do. We survived because these shortcuts persisted; it was the only way to sort through a large number of stimuli without getting overwhelmed. Without them, we would stand frozen — cataloguing, appraising and calibrating — and timely action would be no longer in question. (Cialdini, 2025) We must treat our propensity for making emotion-fueled decisions as a design gap and integrate it into our cyberspace. This is the only way to close the difference between our judgment of best action and the actual safest action.

Some cities have carefully designed the movement of traffic in urban areas. They have considered the design of road demarcations in their thickness and color, the shape of junctions, the obstacles in the road and so on. Urban planners did this in the Netherlands by establishing different stylistic categories of roads, according to their different speed limits, an idea which they referred to as self-explaining roads. (Zhou et al., 2021) However, the most compelling insight when it comes to mapping road safety onto digital safety might be this: the greatest strides were made by designing roads to appear more dangerous than they actually are. Automobile safety researchers found that when traffic junctions look more complicated, drivers take more caution, and the safety of the junction is improved. (Adams, 2001) Interestingly, a traffic junction which is actually difficult, one in which several close calls occur, will make the surrounding junctions safer, because drivers tend to be more careful having exited that junction. This effect is so significant, that making one dangerous junction safer will increase the safety of that particular junction; however, the accident rate in the area will, over time, return to original levels, because the danger of surrounding junctions will slightly increase. (Adams, 2001)

Omitting pedestrian lights at crossings forces drivers to slow down and look for people looking to cross the road. Similarly counterintuitive, obstacles can be very beneficial — a wide, flat unobstructed road will often tempt drivers to break the speed limit.

If we are successful in designing our roads well, the first instinct of the physically and mentally sound person should generate a productive response in the machine and a safe manoeuvre on the road. If we are successful in designing our cyberspace well, we can create a similar compatibility between sane instinct and productive action. If we cannot get rid of our cognitive shortcuts, we must find a way to make the security landscape intuitive for them, or very, very unintuitive when needed.

This orientation has the potential to vastly aid family offices and HNWIs who are not subject to firmwide digital security training to catch up to their commercial counterparts. More significantly, it has the potential to help the cybersecurity aware individual who is still getting caught off guard in meticulously prepared, stunningly executed phishing attacks. It is an orientation which addresses the fundamental cultural weakness Hannah Arendt established in "Eichmann in Jerusalem: A Report on the Banality of Evil". Everyone thinks that they will recognise evil when they encounter it, but Arendt explained how evil can be ordinary in appearance, and how it can lack the dramatic, villainous traits we expect it to have. Everyone thinks that they will recognise fraud when they encounter it, but in truth it will not be obviously sly or monstrous, it will be mundane and "banal", yet dangerous all the same.

© 2025 Baker & McKenzie | 3

Bibliography

Adams J. "Risk: The Policy Implications of Risk Compensation and Plural Rationalities". Routledge; 2001. Accessed 11 June 2025. https://john-adams.co.uk/wp-content/uploads/2017/01/RISK-BOOK.pdf

BakerWorld. US Cyber Factsheet: CIRCIA, NIS2, SEC, NY, HIPAA, NERC and FTC. BakerWorld; [year unknown]. Accessed 11 June 2025. https://whem.bakerworld.com/global/knowhow-whem/Global/ITCommunications/US%20Cyber%20Factsheet%20CIRCIA,%20NIS2,%20SEC,%20NY,%20HIPAA,%20NERC%20and%20FTC.pdf

Bloomberg L.P. Cybersecurity Single Biggest Risk to Family Offices [panel discussion]. Bloomberg Family Office Summit; 27 March 2025; Hong Kong. Jason Lau, Global Board of Directors, ISACA and General Partner an Cofounder, Hanaco Ventures, panellist. Accessed 11 June 2025. https://www.bloomberg.com/news/videos/2025-03-28/cybersecurity-single-biggest-risk-to-family-offices-video

Cialdini RB. "Influence: The Psychology of Persuasion". Fifth ed. Pearson; 2025.

CropInk. 70+ eCommerce Fraud Statistics [2025]: Trends, Data, & Facts. CropInk. Published 2025. Accessed 11 June 2025. https://cropink.com/ecommerce-fraud-statistics

Deloitte Touche Tohmatsu Limited. "The Family Office Cybersecurity Report, 2024". Deloitte; 2024. Accessed 11 June 2025. https://www.deloitte.com/content/dam/assets-shared/docs/services/deloitte-private/2024/summary-family-office-cybersecurity-report-2024.pdf

DHL Customer Solutions & Innovation. "The Logistics of Luxury: Unveiling Luxury Supply Chain Opportunities for Success". DHL; 2024. Accessed 11 June 2025. https://www.dhl.com/content/dam/dhl/global/csi/documents/pdf/glo-csi-logistics-of-luxury-whitepaper.pdf

Lerner JS, Keltner D. "Fear, anger, and risk." J Pers Soc Psychol. 2001;81(1):146-159. doi:10.1037/0022-3514.81.1.146. Accessed 11 June 2025. https://fbaum.unc.edu/teaching/articles/Lerner-2001-FearAngerRisk.pdf

Plassmann H, O'Doherty J, Rangel A. "Orbitofrontal cortex encodes willingness to pay in everyday economic transactions." J Neurosci. 2007;27(37):9984-9988. doi:10.1523/JNEUROSCI.2131-07.2007. Accessed 11 June 2025. https://www.jneurosci.org/content/27/37/9984

Statista. Luxury e-commerce — statistics and facts. Statista. Published 2025. Accessed 11 June 2025. https://www.statista.com/topics/8247/online-personal-luxury-goods-market/

Zhou X, Li J, Chen S, et al. [Title of the article]. Cognit Res. 2021;6(1): Article 81. doi:10.1186/s41235-021-00281-6. Accessed 11 June 2025. https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-021-00281-6

© 2025 Baker & McKenzie | 4

Contact us

Marnin J. Michaels
Partner
marnin.michaels@bakermckenzie.com

© 2025 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.