STEVEN WATSON

RISK, BENEFITS, AND THE AFFECT HEURISTIC IN SECURITY BEHAVIOURS

Most of us like to think of ourselves as honest and law-abiding. Yet, the prevalence of online piracy (or, more formally, unlawful file-sharing) shows that many of us are perfectly willing to act contrary to the law.

My colleagues and I reviewed the extant literature on the determinants and consequences of unlawful file-sharing to understand why so many people were willing to break the law in this way. We found a diversity of reasons. These included people's desire for new content, personal attitudes toward and moral arguments about unlawful file-sharing, and their beliefs about social and cultural norms regarding the acceptability of unlawful file-sharing.

For a long time, the predominant approach of legislators and industry had been to try to reduce unlawful file-sharing by attempting to increase the perception of how legally risky this behaviour was, for example, through lawsuits or the introduction of punitive legislation. This focus on risk proved to be ineffectual. There are lessons to be learned regarding why this focus on risk was not effective in changing unlawful file-sharing behaviour, which transfers to numerous security contexts.

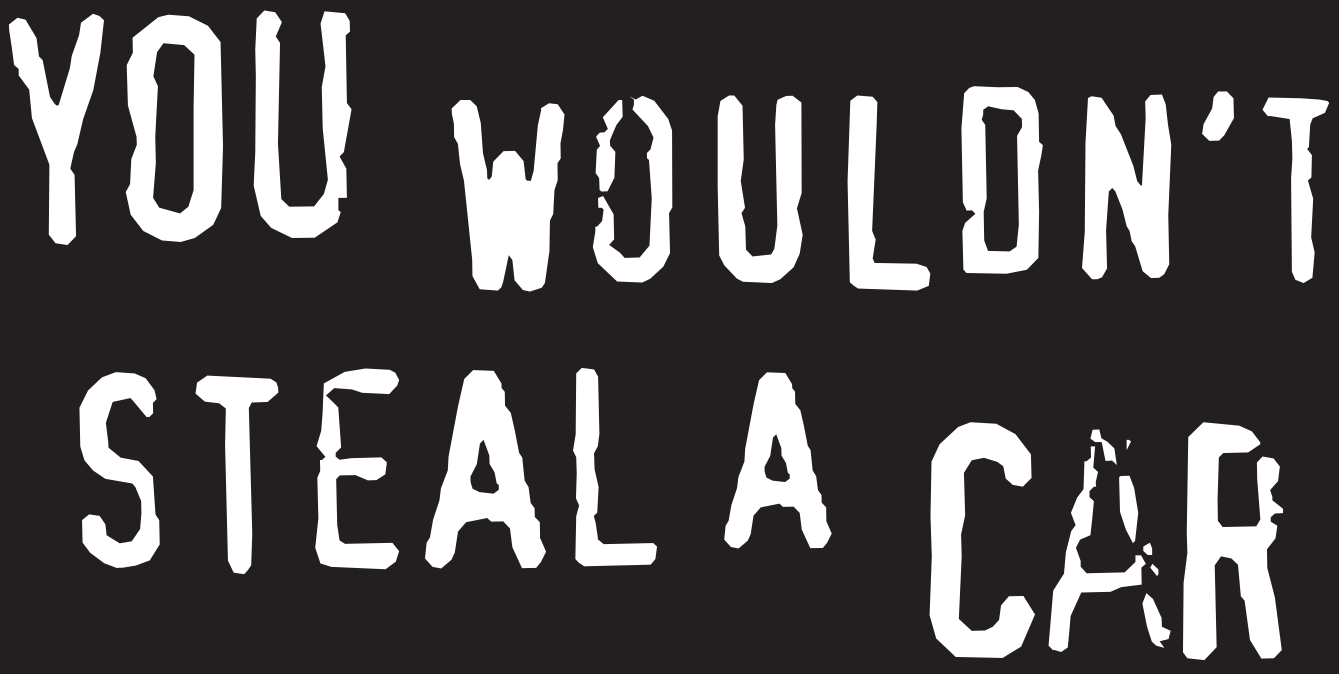
Risk is at the heart of many attempts to understand security-related behaviours and attempts to try to enact behaviour change to adhere to better security behaviours. The rather sensible underlying logic is that if people understand why their behaviour could undermine their own or others' security, they are less likely to do it. Thus, educating people about the risks associated with their behaviour, or increasing perceptions of how risky their behaviour is, should lead to people adopting more secure behaviours.

> **It was not legal threats that began to reduce the unlawful file sharing of music, but the availability and affordability of Spotify and iTunes.**

However, there are reasons to be cautious here. Sometimes we engage in behaviours because of the perceived benefits they bring, and we do not necessarily think too much about potential negative consequences. This was one of the key findings of my colleagues and I when investigating why people unlawfully download copyrighted files. They do not think of the associated legal risks when engaging in unlawful file-sharing behaviour, but rather, they think of the personal benefits of owning the downloaded files themselves.

Similar logic is likely to apply to security behaviours. For example, when selecting a new password for a website, people may know that a weak password brings risks, but at that moment, they are more concerned about their ease of access and so may recycle a weak password they use on multiple websites. If we wish to change this negative user behaviour, we need solutions that address the benefits motivating these users' poor security behaviours. After all, it was not legal threats that began to reduce the unlawful file-sharing of music, but the availability and affordability of Spotify and iTunes; legal services that met the perceived benefits of unlawful file-sharing in terms of diversity and availability of content. Therefore, if we want people to use strong passwords, they probably need a convenient, easy-to-use solution as much as they need a warning that their security behaviour is suboptimal.

There are additional challenges that come from instances where individuals are more focused on benefits than they are on risks. That is because when an individual is focussing on the perceived benefits of poor security behaviours, this can actively undermine the effectiveness of any risk-based interventions via the affect heuristic.



"You Wouldn't Steal a Car" is the first sentence of a public service announcement, part of the 2000s anti-copyright infringement campaign 'Piracy. It's a crime.' It was created by the Federation Against Copyright Theft and the Motion Picture Association in cooperation with the Intellectual Property Office of Singapore.

THE AFFECT HEURISTIC

The affect heuristic refers to the observation that how risky people think something is depends on how they feel emotionally about an action and its outcome. If they feel positive about the action or its consequence, then they tend to underestimate the associated risk. Conversely, if they feel negative about an action, then they tend to overestimate the associated risks. In reality, the two need not be associated at all, and often there is a positive correlation; great rewards often follow great risks.

This is why the affect heuristic is useful. It motivates us to ignore risk for beneficial outcomes or disincline taking even small risks for scant benefit. For example, this is a reason why we fall for email frauds. If an online fraudster offers us something we value greatly (such as money or the promise of romance), we tend to overlook the warning signs that offers may not be genuine.

TWO SYSTEMS OF THOUGHT

The affect heuristic is an example of what psychologists refer to as a System 1 process. System 1 processes are fast, automatic, and effortless. They contrast with System 2 processes which refer to deliberate, effortful cognitive work to think through a problem. Not surprisingly, people prefer to avoid having to use System 2 unless they have to. 'Going with our gut' and following the affect heuristic saves us a lot of time and energy and is adequate for most day-to-day decisions. However, allowing our affective processes free reign to make high-stakes decisions is a significant gamble, especially within security settings.

AFFECT HEURISTIC IN SECURITY SETTINGS

Security professionals in a range of settings must decide whether individuals, groups, or information pose a level of risk that should be acted upon. Without structured tools to guide risk assessment, errors based on security professionals' positive or negative feelings about groups or individuals are likely.

Such biases can also be created by even a small number of well-publicised events, as is likely when considering rare but high-impact scenarios such as terrorism. Fortunately, we do know of ways to reduce reliance on affective processes when making risk judgements.

GETTING MORE ACCURATE JUDGEMENTS

Time pressure

Time pressure increases reliance on affective processes. This pressure is one reason having mandatory tools, such as risk assessment tools, to force System 2 thinking can be helpful. It forces time-poor professionals to think through problems and not rely on gut instinct when it may not be appropriate.

Perceived anonymity

Perceived anonymity also increases affective thinking because the decision-maker assumes consequences of errors are unlikely to be traced back to them. Anonymity, therefore, lowers the risk to the individual and may reduce the requirement to engage effortfully with the risk assessment process.

Trust

When we trust organisations or groups, we also tend to perceive lower risk and rely on the affect heuristic. It is, therefore, important that trust is not misplaced.

Prevention strategies

A focus on prevention strategies (prioritising identifying as many risks as possible, even if this means some identified risks are not real) over promotion strategies (prioritising identifying only real risks) discourages affective processing of judgements. This is often appropriate in risk-averse security settings.

Presentation of information

People respond to changes in how information is presented. If the benefits of a course of action are emphasised, then the risks are assumed to be lesser. If the risks are emphasised, then the risks are believed to be greater. This means the affect heuristic can be exploited to enhance accuracy if the motives that underpin the behaviour are known.

> **Allowing our affective processes free reign to make high-stakes decisions is itself a significant gamble, especially within security settings.**

Therefore, it is crucial to understand whether a behaviour is 1) primarily performed in order to reduce risk (high-risk salience) or 2) to gain a particular benefit (high-benefit salience). Risk salient behaviours should be promoted by reinforcing the level of risk, whereas benefit salient behaviours should be targeted by addressing the identified benefits.

For example, highlighting the dangers of not wearing a seatbelt can be effective because people only wear seatbelts because they lower risk. On the other hand, highlighting the benefits of condom use for safe sex is not always effective due to people's focus on pleasure, not risk. Hence, it would be more effective to make condoms that make sex more pleasurable. Or, returning to unlawful file-sharing, by developing legal alternatives that offer the choice and functionality of unlawful alternatives.

CONCLUSION

We know that individuals may make inaccurate judgements because of their subjective feelings, but we also know that setting up good organisational systems can mitigate these issues. Having accountable decision-making via structured risk assessment tools and providing professionals the time required to complete these correctly can lead to superior decision-making. This means more accurate risk judgements, fewer missed threats, and enhanced security for everyone.

We also know that changing poor security behaviour only through increasing perceived risk is unlikely to work in all scenarios, especially when poor security practice confers tangible benefits. We should aim to develop solutions that address these perceived benefits and make improved security as simple and pleasurable as possible.

Dr Steven Watson is an Assistant Professor in Psychology at the University of Twente. His research is in applied decision making, especially within security and legal contexts.