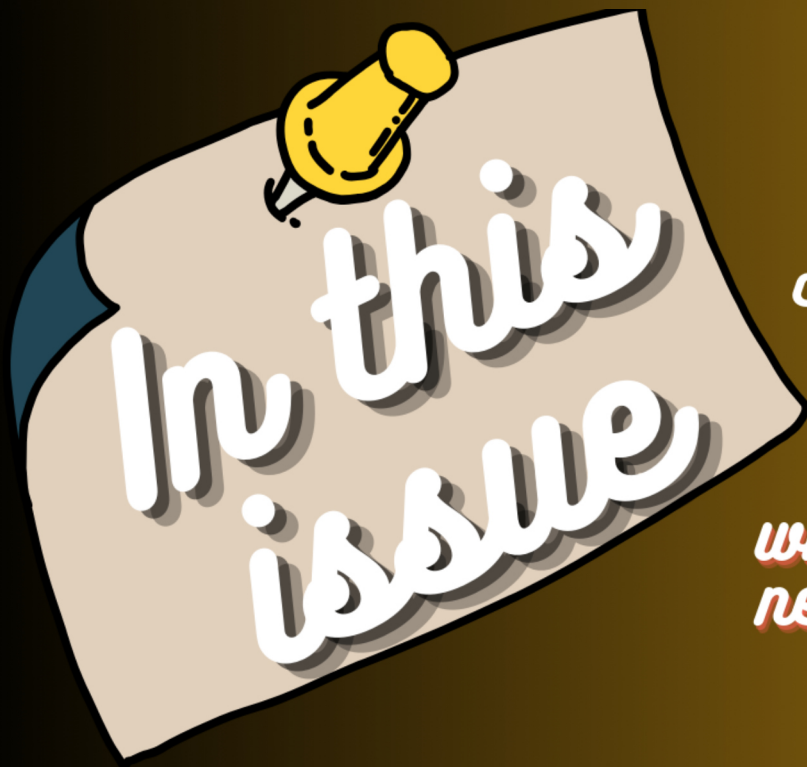


Supporting the growing field of cyber-criminology and seeking to future proof the cybercrime fighting work force.



Cyber-criminology Magazine

Issue 1 - May/June 2024



*some fun with a
criminology themed
crossword*

*why cybersecurity
needs Criminology*

*cybersecurity measures
enhanced by applying the
routine activity theory*

*cyber security & risk expert
Mike Holm
with his column
"Smooth Sailing Cyber Security"*

rational choice theory & cyber security

.... and much more!

incognito criminology

SUPPORTING THE GROWING FIELD OF CYBER-CRIMINOLOGY AND SEEKING TO FUTURE PROOF THE CYBERCRIME FIGHTING WORK FORCE.

Issue #1 - May/June 2024

EDITED BY
A TURNER



Independently published by www.empressbat.com



Mike Holm

Shakira Memorey

Nyalek Gatwech

Amanda-Jane T

contributors

*Submissions welcome.
Please email the team at
incognitocriminology@gmail.com*



contents

<u>From the editor</u>	6
<u>Smooth Sailing Cyber Security column</u>	8
<u>Introduction to cyber-criminology</u>	12
<u>Cybersecurity needs criminology</u>	13
<u>Crossword</u>	14
<u>My cyber-criminology journey</u>	16
<u>Intersecting disciplines</u>	18
<u>Rational choice theory and cybersecurity</u>	19
<u>Cyber-criminology, what is that?</u>	20
<u>Using criminology to design cybersecurity awareness</u>	22
<u>Deepfake voice cloning as a service</u>	23
<u>Cybersecurity measures enhanced by routine activity theory</u>	24
<u>Five tips for cyber-criminology students</u>	26
<u>Solution to crossword</u>	27



Welcome to **Incognito Criminology!**

This is an independently published magazine that seeks to support the growing field of cyber-criminology and future proof the 'cyber-crime fighting' workforce.

BEHIND THE MAGAZINE

Why Incognito Criminology? Because, 'behind the scenes, in the shadows, intelligence, cybercrime, criminology, cybersecurity, physical security, personnel security, privacy, research, and careers information to help students', was not a snappy title!

Cyber-criminology as a discipline is fairly new, having been spoken about from around 2007 but still not widely adopted. With its focus on applying criminology theories to cybercrime it is an essential aspect of cybersecurity.

I chose 'Incognito' as part of the magazine name, because just as cybersecurity needs criminology, privacy also needs to be an integral part of a cybercrime fighters arsenal.

The logo shows stylised people together (to show that we need to work together to fight cybercrime), a mortarboard (to illustrate academics, students and studies), resting on a book (for research and news), inside a shield (for security and law enforcement) and tied with a ribbon banner (to show privacy tying everything together).

Why did I start this magazine? Cybercrime is not going away any time soon, so it is important that as a community we enable the creation of a long term future proofed sustainable cybersecurity workforce. This means taking onboard new ideas, exploring emerging technologies and research, and making information accessible to those with an interest in this field. I am passionate about supporting students and those new (or changing careers) to cybersecurity, security, cyber-criminology, investigations, privacy, or intelligence.

I want to give students, academics, researchers, and industry a voice without red tape, a safe place where we can share information, articles the cohort has written, interesting research, upcoming events, raise the profile and importance of cyber-criminology, support cybersecurity awareness in the community, and have some fun while doing so.

🔍 In a world where cybercrime is rapidly evolving, staying ahead is not a luxury it's a necessity. We need to embrace new theories, practices and possibilities to enable a future proofed, sustainable, cybercrime fighting workforce.



Amanda-Jane T
www.empressbat.com



Smooth Sailing Cyber Security

Mike Holm - cybersecurity and risk expert

Many of the cyber security professionals around the globe are concerned about [third-party risk](#). What exactly is that, and why should you care? Personally, I like to apply what I consider to be a layer of common sense across these sorts of things, but I feel that I'm very privileged to constantly learn from some of the very best cyber security professionals in Australia and nearby, so perhaps what I assume is common sense is actually their knowledge "bleeding through" me! So let me impart some of that knowledge I've accumulated, and hopefully you can benefit from it as I have done.

Let's consider a small business, a hairdressing salon. Typically the team interacts directly with clients of course, although in order to service those clients, there's very likely a CRM (customer relationship management system) to handle appointments, hold client information, and possibly even manage a pipeline of new clients. Additionally, there'll be an accounting system to handle revenue from clients, and payments for staff salaries, suppliers and other operating costs, and to prepare the salon's [Business Activity Statement](#) (the Australian government's method of collecting company tax). It's also practically an expectation now that the salon maintains a presence on social media, so let's include Facebook and Instagram for argument's sake. The salon would probably maintain a good old-fashioned website as well, unless they're content solely relying upon their social media pages for marketing purposes.

Now consider the *information* held in each of those systems. The accounting system will hold banking details for staff and suppliers. The CRM will hold customer information such as email and phone contacts. Ask yourself “If my email address, phone number or banking details were included in those systems, and the salon’s information systems were targeted by an attacker who *stole my information*, how would I be affected?” In 2022 when [Optus suffered a data breach](#), there were *ten million individuals* affected, so odds are you’ll have first-hand knowledge of the process of replacing pieces of personal identification like driver licences, or you’ll know someone who went through it.

As members of the public, we have an expectation that businesses and governments protect our personal information appropriately. For the sake of brevity I won’t go into the regulatory requirements of this, suffice to say the [Privacy Act \(1988\)](#) has had numerous amendments over the years, most notably the Notifiable Data Breaches scheme in 2018. This affords us reasonably good protection assuming everyone follows the rules, noting [fines of \\$50M can be imposed \(or higher in some cases\)](#), with some exceptions.

Back to our salon example, and the accounting system is most likely a [cloud-based system](#) the salon pays a subscription to. It seamlessly integrates with the point-of-sale system, itself possibly another cloud-based subscription service, and it “automagically” pays staff directly into their bank accounts according to timesheet information. To the salon, it’s relatively low cost, easy to use, and critical to their business. However it is a *third party supplier* to the salon, which means the salon can’t directly control its operation.

Now the question “if an attacker stole my information from the salon, how would I be affected” is more complicated. What if the attacker stole my information from the company that operates the accounting system, along with many other individuals’ information, from other salons and all kinds of businesses? Surely that would be a more lucrative bust for the attacker?

This is exactly the kind of thinking an attacker may employ to [target weak points in the supply chain](#) from third parties. The cloud-based accounting system used by the salon is by its very nature highly accessible, from all around the globe. This increases the attack surface, lowering the cost of a successful attack. Remember from the attacker’s point of view, this is about the *information held in the accounting system*, not the system itself. Before we had technology, that salon owner would have simply locked the accounting ledger physically in a safe to protect it from theft, and the attacker would have needed physical access to the salon, and safe-cracking skills to steal it!

Does this make cloud-based accounting (and other) systems unsafe? Not necessarily, however any system or structure can have weak points. For example, one very common attack is the [phishing scam](#), in which the attacker tricks the victim into disclosing their login credentials, allowing the attacker access to the victim's private information. Although many technology providers use mitigating controls such as [multi-factor authentication](#), sometimes these controls are optional, and can even introduce further weaknesses. Keep a close eye on *Incognito Criminology* and other [trusted sources such as the Australian Government ScamWatch](#) to stay up to date on the latest cyber attacks.

What does this mean for your business, and your supply chain? You'll need to be aware of and close off the weak points, and have a plan in case the worst should happen. This could be included in your overall [incident response plan](#), which should cover as many eventualities as possible to minimise the impact of all kinds of incidents, not just those involving technology. Cyber security risk is just like any other risk, it requires analysis of threats, an understanding of the impacts and their likelihood, and appropriate risk treatments to keep your business operating. Without guidance, this process can be quite daunting. A mentor once told me, "The attacker's job is easy; just find one weakness. Our job is to find *all the weaknesses* and plug them before the attacker exploits them!"

In our third party risk discussion example here, the salon owner would begin by figuring out who the third parties are, how they're relied upon, and how vulnerabilities in their systems and processes could be exploited by attackers to compromise the salon's business. In *Smooth Sailing Cyber* and elsewhere in *Incognito Criminology* we'll delve further into that process, but for now why not start a "cyber champions" club in your workplace? For an easy start, spend a few moments discussing the activities you regularly carry out in your jobs, for example "sending mailouts to our clients' email addresses" or "running the payroll for the office". For each activity ask the question, "What information is handled or stored for this activity?" For example "customer email addresses" and "staff bank account information". You've just carried out one of the first steps in managing risk: *identify your assets!*

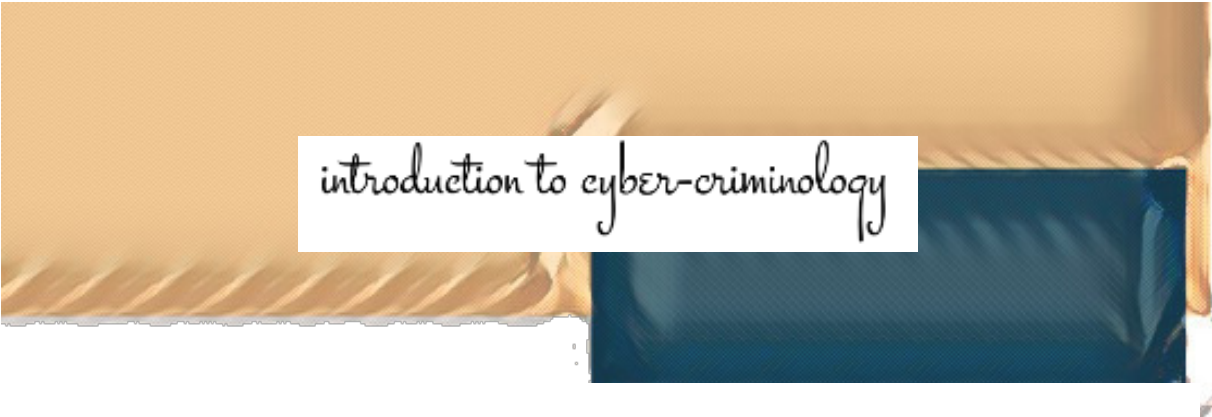
If you really can't wait until the next issue of *Incognito Criminology* to learn more, the [Australian Cyber Security Centre](#) has great advice for small businesses looking to manage their cyber security risk.

Bio

Mike is a cyber security and risk expert with over 20 years in the field. Initially in technical roles such as threat detection, he transitioned to security projects, governance, risk, and compliance. With specialist and management experience in the finance, higher education and CERT sectors, he has also managed teams in the SME sector, gaining insight into their specific security needs. Mike has always emphasised the crucial role people have in managing cyber risk, advocating for enhanced security awareness and education. On those rare occasions when Mike's laptop is closed, you might find him walking his dogs, enjoying a coffee with his husband or sailing on The Bay.



Smooth sailing cyber will be a regular column from
Mike Holm, Cyber Security and Risk Expert



introduction to cyber-criminology

It is believed that the field of cyber-criminology started with Professor Karuppanan Jaishankar¹ whose research and commentary on criminology and cybercrime included new theories on criminal behaviours in cyberspace. In 2007, Professor Jaishankar proposed the application of the *Space Transition Theory* to cybercrime. He used this theory to help explain the behaviours of people as they move from physical space to cyber space and how this may increase their inclination to commit crime.

Crimes in cyberspace are as diverse as those committed in physical space. In Australia, for example, cybercrime refers to crimes directed at computers or other information communications technologies, and those where computers or other information communications technologies are an integral part of an offence. This is a huge umbrella of crime types and it is therefore fitting that there is a criminology discipline devoted to it.

Cyber-criminology looks at the human factors of cybercrime, including victimisation, criminals, motives and methods. It is an essential part of cybersecurity, as it is easier to mitigate, protect against, and educate others on cybercrime when the motives and methods are understood.

Still a relatively new discipline, cyber-criminology enhances an increased understanding of the crime, victims, and methods which enables a more informed and strategic approach to cybersecurity.

1. Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology*, 1(2), 7-9.

cybersecurity needs criminology

Understanding the motivations, methods, and victims of criminals using technology to commit crime is an important aspect of operational cybersecurity.

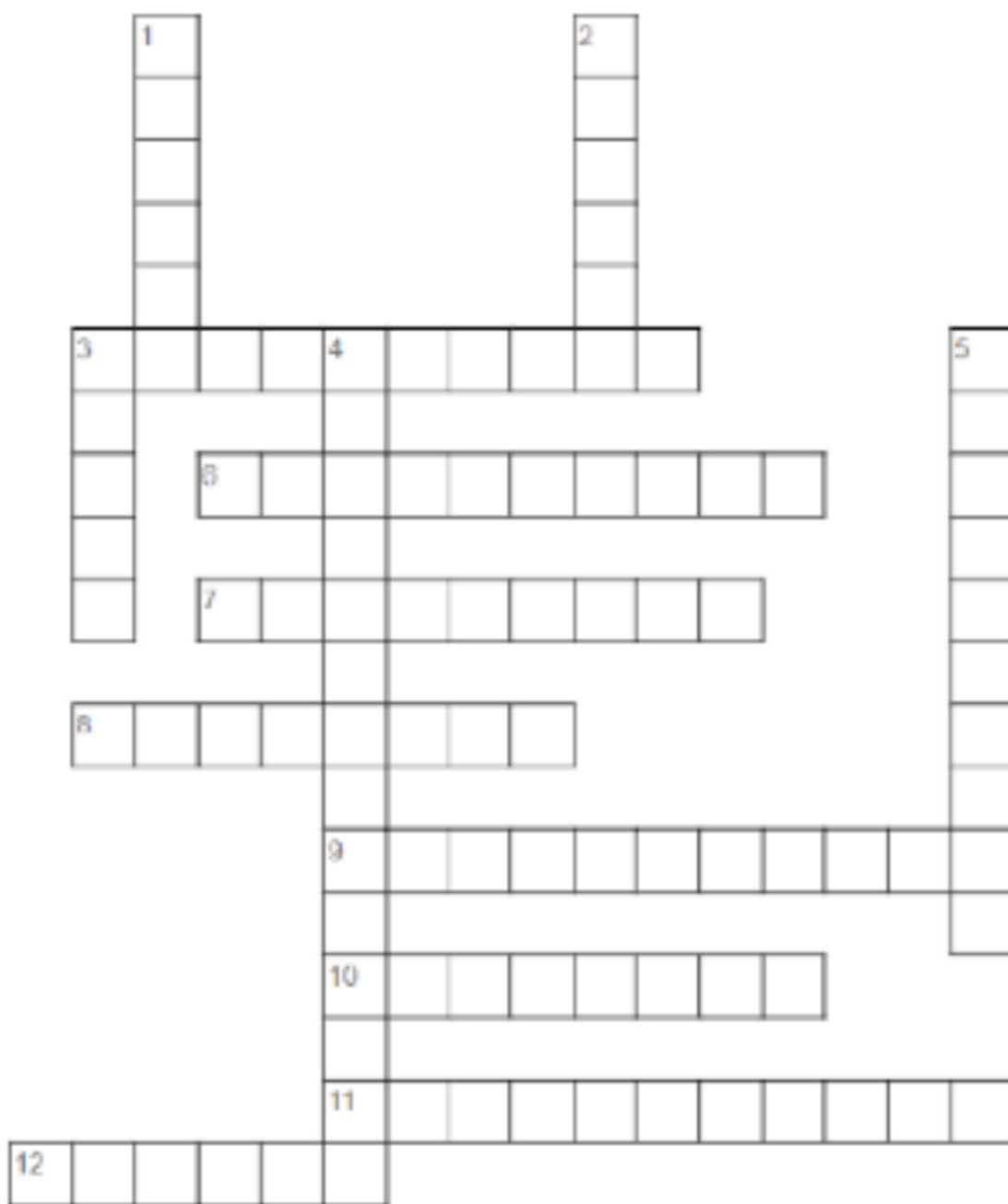
Cybersecurity is more than tools, networks, and stopping phishing. Internet connected devices, critical infrastructure, and finances are all tied up in the twenty-first century digital environment.

To better protect against network intrusion, Nation State sponsored cyber threats and cyber enabled fraud, a cybersecurity professional should not ignore the human aspects to the crimes.



Crossword

Enjoy this criminology themed crossword, answers can be found near the back of the magazine



Across

3 Criminal activity that involves the use of computers, networks, or digital technologies.

6 The use of punishment or other measures to discourage individuals from engaging in criminal behaviour.

7 A sentencing option that allows offenders to remain in the community under supervision instead of being incarcerated.

8 Behaviour that violates social norms or expectations.

9 The branch of the criminal justice system responsible for the supervision and rehabilitation of offenders, including prisons, probation, and parole.

10 A person who commits a crime

11 The scientific study of crime, criminals, and the criminal Justice system.

12 The supervised release of a prisoner before the completion of their sentence, subject to certain conditions and restrictions.

Down

1 A systematic explanation or framework for understanding the causes and dynamics of criminal behaviour.

2 A person who suffers harm, injury, or loss because of a criminal act.

3 An act or omission that violates the law and is punishable by the state.

4 This theory insists that crime is calculated and deliberate. (2 words)

5 The tendency for a convicted offender to reoffend or engage in criminal behaviour after being released from punishment or supervision.





my cyber-criminology journey

By Shakira M - cyber security intel analyst

When I made the decision to study criminology, I had a very narrow idea of what it would entail. I thought it would equip me with the skills to join law enforcement and I hadn't really considered much else. Upon commencing university, I quickly began to understand the complexities that criminology aims to unpack, which widened my perception of crime extensively. An invaluable skill I gained from my undergraduate degree is the ability to analyse a scenario objectively and critically, whilst also understanding the events and circumstances that led to such offending.

Criminology covers a diverse range of issues and concepts whilst challenging you to become comfortable with being uncomfortable – something that is very important in this field of work and study. The topics that are covered allow you to delve into issues that are only superficially represented in the media, allowing you to consider significant contemporary issues. In undertaking this degree, I have learned a plethora of information about criminological theories, cross-jurisdictional comparative criminology, the role of intersectionality in criminal behaviour and responses to crime, and a lot about sociology. Alongside this, I have learned about what contributes to recidivist offending, and ways in which we can work towards reducing recidivism. The reality of crime prevention and recidivism reduction is no black-and-white issue, unlike the media (and even politicians) would lead people to believe.

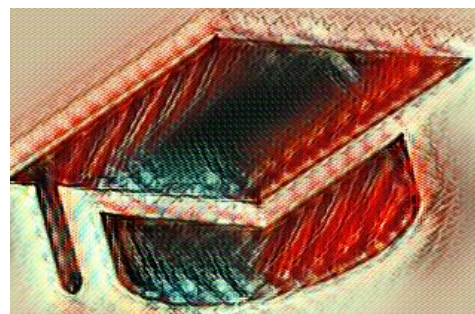
An area of interest for me has always been child protection and child exploitation prevention. The advent of the internet has seen the proliferation of online child exploitation, and industry experts are struggling to keep up with these offences and offenders. Three years into my degree, I almost felt boxed into a pathway of entering corrections or law enforcement. However, given all that I had learned, I wanted further direction, something like a "specialisation". Unlike other degrees, I didn't have a major or minor, instead I learned a lot about such a diverse topic. I was initially enrolled in a four-year degree with an embedded honours year; a Bachelor of Criminology and Criminal Justice (Honours), and I was scared not to see this through. So, when I first learned about the alternative pathway of graduating with a Bachelor of Criminal Justice and then undertaking a Master of Cyber Security (Cyber Criminology), I did not pay much thought to it. I had become set on the fact that I had chosen my degree in year 12, and altering my pathway was intimidating.

So, how did I end up here, studying a Master of Cyber Security and working in a cyber security operations centre? It was about two months after learning about the master's degree that I allowed myself to explore the benefits that cyber security and cyber-criminology would have for someone wanting to work in child protection and child exploitation prevention. I realised that by being scared to alter my degree pathway, I was blocking myself from further knowledge and progression. I started applying for cyber security internships and was able to secure a position with a summer internship program that was specifically looking for students studying criminology and criminal justice. This internship was extremely valuable for me, it provided me with foundational cyber security knowledge and experience that now adds context to my further studies.

What I learned in my undergraduate degree has been extremely beneficial for my understanding of cyber security, because despite the new medium of offending, the offenders and victims are still human. Online offending has increased complexities for crime prevention and responses, and I am happy to say that I am choosing to continue my cyber-criminology journey to help combat cybercrime. Since completing my first internship and commencing my first semester of my master's degree, I have learned so many skills and I have applied this knowledge almost daily: at work, completing assessments, and educating friends and family. What I love about the current pathway I am on is that I can see how what I am doing and what I am learning contributes to change within this industry, which I am so passionate about.

What advice do I have for those wanting to get into cyber-criminology?

- Your university grades may not seem like the most important thing in the grand scheme of your career, but the relationships that you build with your lecturers and their industry colleagues are very important.
- Put yourself out there. Do not be scared to apply for internships or reach out to industry experts. If you do get knocked back from an internship, reach out to the hiring manager or HR team for advice on how you could do better next time.
- Do not be afraid of change.





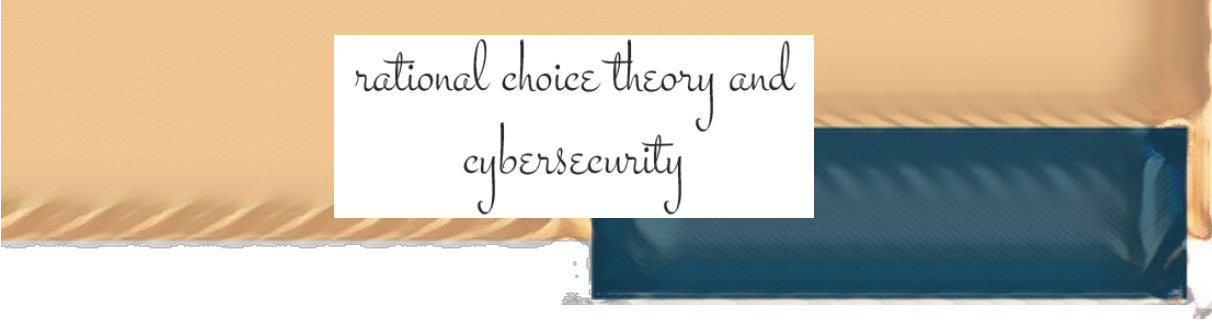
intersecting disciplines

The more technology and cybercrime evolve, and the reliance of interconnected data bases increases, the more vital it is to ensure a seamless intersection of criminology, privacy, and cybersecurity disciplines. Cybersecurity is a critical component of (cyber)crime prevention, and the privacy field adds to this with governance and laws over how personal information is stored, transmitted, and protected. Criminologists examine the methods and motivations of cybercriminals and analyse the vulnerabilities that provide explanations of victimisation.

For example, there is an upsurge of ransomware double extortion, where the cybercrime campaign not only encrypts files, but also steals and holds for ransom personal information. This is a concern for all three fields.

- **Privacy** – where the focus is on protecting personal information and ensuring that individuals have control over their data. As part of ransomware incident response, privacy experts may need to consider if the data exfiltrated during a ransomware incident is personal information and determine if it is a data breach that requires reporting, and if so to whom.
- **Cybersecurity** – where the field is responsible for protecting people, data, and networks from the impact of cybercrime, including helping to safeguard systems from unauthorised access resulting in data breaches. As part of a ransomware incident response, they would need to determine the motives, methods, and vulnerabilities that allowed this malicious campaign to succeed. Cybersecurity professionals would also be responsible for supporting the recovery of networks after such a compromise, and work with privacy teams in regard to potential breaches of personal information due to the ransomware.
- **Criminology** – in looking at the crime motives, methods, and victims, criminologists can form actionable intelligence for cybersecurity professionals and law enforcement to apply to mitigate the impact of cybercrime or support attribution to specific ransomware groups.

To effectively counter cybercrime, there needs to be an Interdisciplinary approach, drawing on skills and knowledge from various fields, including intersecting the disciplines of criminology, privacy, and cybersecurity.



rational choice theory and cybersecurity


Whether committed in cyberspace or physical space, crime has real world motivations and real victim consequences. Cybercrime can be opportunistic, but it can also be carefully thought out, with targeted victims, business structures, and deliberate actions.

Rational choice theory suggests that a criminal, after weighing the potential benefits and costs of their actions, makes a calculated and conscious decision to commit the crime. Although not all cybercrime is considered and calculated by those committing it, there is opportunistic cybercrime after all, looking at state sponsored threat actors or cybercrime as a business for example, there is a strong match to the rational choice theory.

Rational choice theory considers how criminals assess the potential rewards and perceived benefits, such as financial gain, recognition from their nation, or personal or ideological objectives being met, against the perceived costs to commit the crime. Criminals involved in cybercrime who carefully evaluate the potential risks, including legal and financial consequences, or retaliation from other criminals or state sponsored actors, against the perceived gain, prior to committing the crime, fit into this theory.

How does rational choice theory help in assessing cybercrime, or supporting cybersecurity efforts?

Understanding motivations behind cybercrime, in whatever criminology theory they fit, helps inform cybersecurity mitigation and awareness measures. With cybercrime types that fit the rational choice theory - If cybersecurity mechanisms make the risk and cost to commit the crime far outweigh the benefits, it may help harden communities against that crime.



cyber criminology?

“what is that?”

By Nyalok Gatwech- cyber security awareness advocate and analyst

As a humanities enthusiast and curiosity-driven learner, I was initially stumped as to what I wanted to do and study leaving high school – a feeling I found to be all too similar amongst my peers. I decided to study a Bachelor of Arts which allowed me the flexibility to explore a range of subjects/disciplines from Globalisation & Development in Post-Colonial Societies to Archaeology. I completed an extended major in Criminology with the intent of pursuing a career within the justice system or a role which I thought would be intrinsically tied to my studies of social science. At this time I was motivated to pursue Criminology given the centrality of understanding offender behaviour, victimisation and the phenomena of crime.

My interest was initially peaked to the notion of cybersecurity, technology and online spaces when I took an elective course on Global Security. Having being introduced to this new concept of Cyber Criminology, I became intrigued by the application of social science perspectives and criminological theory in security and to technology more broadly.

With an established passion for Criminology, I've since continued to explore this area through the Master of Cyber Security (Cyber Criminology) program. This program has enabled the exploration of criminological principles, as it relates to its application to technology and online spaces. It has also reinforced the importance of diverse thought within such a dynamic industry. Interdisciplinary approaches in cybersecurity are imperative, whether you are considering risk, technical analysis, culture or operational security. This bodes similarly within Criminology and the world of cyber, given the need for understanding wider political and social factors that play into addressing offending behaviour and threat actors.

How applicable are these skills in the world of cybersecurity?

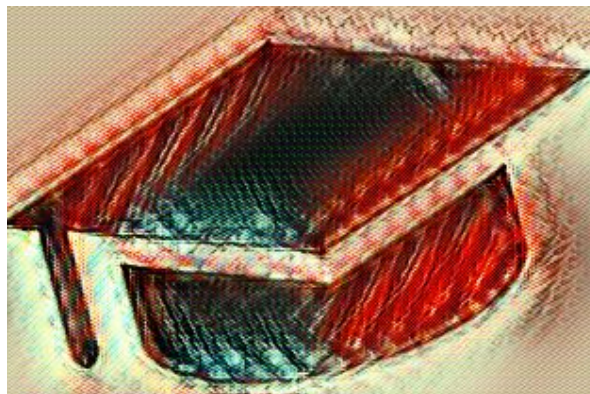
As I've continued my studies, I've been more motivated to begin a career in cybersecurity, knowing that the skills I've developed in my studies of Criminology are needed within the cybersecurity profession. By combining social science skills and perspectives with my newly acquired knowledge of cyber security, I will continue to support cybercrime prevention efforts. Criminological understandings are essential to cybercrime prevention and detection to secure systems, protect users and contribute to creating a safer space for everyone online.


So, what's the experience been like so far?

Having had the privilege to gain experience in different areas of cybersecurity – including within a cybersecurity culture team and cyber security operations centre – I've broadened my perspectives of preventative and responsive aspects of criminology that extends to cybercrime.

I applied for cybersecurity internships not clearly knowing what they would entail but thought it best to start somewhere. I was worried that my background in Criminology wouldn't suffice to fulfil the roles I was applying for. However, was pleasantly surprised by the demand that employers have for both Criminology students and students from non-technical backgrounds.

So yes, there's a place for criminology students within the cyber security industry. Cybersecurity is far from black and white – which can also confidently be said about Criminology as a discipline and in practice.





using criminology to design
cybersecurity awareness

Cybersecurity awareness training can struggle to stay relevant with emerging threats, not support a positive cultural change, and may concentrate on what a person shouldn't do without explaining why.

Instead of directing employees to not click links, and be suspicious of all emails, or to not download anything from the internet, help them understand criminal motivations and behaviours, and why they need to be cautious. Cybercrime keeps evolving and cybersecurity measures need to evolve with them. Instead of relying on directives of what not to do, support employees to understand better how to identify cybercrime acts themselves.

Explaining the motivators of cybercrime, rather than merely pointing out specific cybercrime examples (phishing, ransomware etc) can help employees gain a better understanding of cybercrime, which enhances their ability to effectively identify and stay vigilant from emerging cyber based threats.

Integration of criminology theories into cybersecurity awareness programmes can help organisations develop more effective strategies to help employees recognise and mitigate cybercrime.

Incorporating criminology theories such as **Routine Activities Theory** for example, in cybersecurity awareness and culture programmes, allows for specific threats facing that entity or industry to be addressed. Employees can be made aware of various tactics techniques and procedures used by and

being evolved by criminals to steal credentials, scam them of funds, or compromise networks. This also empowers employees to think outside of the 'don't click the link' mentality.

The **Strain Theory** could also be applied to cybersecurity awareness initiatives. This criminology theory suggests that societal pressure to achieve success and be rich, coupled with limited legitimate opportunities for achieving it, can create strain. In simple terms, the theory posits that individuals experiencing this strain may turn to crime to achieve their goals. How could this apply to cybercrime? How would this help cybersecurity awareness measures? This theory can be used in conjunction with other frameworks to develop initiatives for raising awareness with employees about being aware of potential underlying social and economic inequalities that may contribute to insider threats or externally perpetrated cybercrime.

Supporting cybersecurity awareness and culture uplift the **Social Learning Theory** which suggests that people learn from observing and applying the behaviours of others. The theory suggests people learn from observing the behaviours of others and are therefore more likely to engage in crime if their attitudes and behaviours have been shaped in socialisation (with family, peers, social media, etc) towards criminal activities.

Conversely this theory demonstrates the importance of positive role models and strong social networks in preventing criminal behaviours. By leveraging this concept, organisations can introduce security champion programmes to encourage positive peer influence regarding cybersecurity awareness and being an active participant in security rather than just doing what they are told.

Applying criminology frameworks to cybersecurity awareness can support organisations to better explain cybercrime, and instead of directives to not do something, helps arm employees with a better understanding of cybercrime methods and motives, so their understanding can keep evolving as cybercrime evolves. Using criminology theories when developing cybersecurity culture initiatives can encourage a culture of understanding of and vigilance for cybersecurity with all employees.

DEEP FAKE VOICE CLONING AS A SERVICE

It is no longer enough to raise awareness about financial fraud and credential theft via emails, with emerging Deep Fake technology these crimes can be committed via video and audio cloning.

Various forums on the dark web have posts from criminals requesting to buy, or offering for sale, voice cloning-as-a-service (also known as VCaaS).

These services provide very convincing voice clones, and are being used for cyber enabled financial fraud and other cybercrime types.

Stay alert!

cybersecurity measures enhanced
by routine activity theory



It can be helpful to consider criminology theories while ascertaining gaps in cybersecurity, and the potential for cybercrime activities targeting an individual or organisation.

For example **Routine Activity Theory**, developed by Marcus Felson and Lawrence E. Cohen in 1979¹, posits that crime occurs when three elements converge:

1. MOTIVE - there needs to be motive/motivated offenders
2. TARGETS - there needs to be suitable targets
3. ABSENCE OF GUARDIANSHIP - there needs to be an absence of capable guardianship.

When applied to cybersecurity Routine Activity Theory points to cybercrime occurring when there are motivated attackers, vulnerable systems, processes, or people (suitable targets), and inadequate security measures, mitigations, or end user awareness

1. Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.

(absence of capable guardianship). The suitable target could be individuals or organisations with weak email security protocols or employees who are not adequately trained to recognise malicious emails such as phishing attempts. The absence of capable guardianship might refer to the lack of effective cybersecurity tools such as email filtering systems or monitoring applications, under resourced cybersecurity teams or insufficient cybersecurity awareness training programs within the targeted organisation.

By applying Routine Activity Theory to cybersecurity, researchers and cybersecurity practitioners can better understand the conditions that contribute to cybercrime and use this knowledge to develop effective strategies to mitigate risks focusing on addressing the factors related to motivated offenders, suitable targets, and guardianship.



we need to future proof a
sustainable diverse cybersecurity
workforce

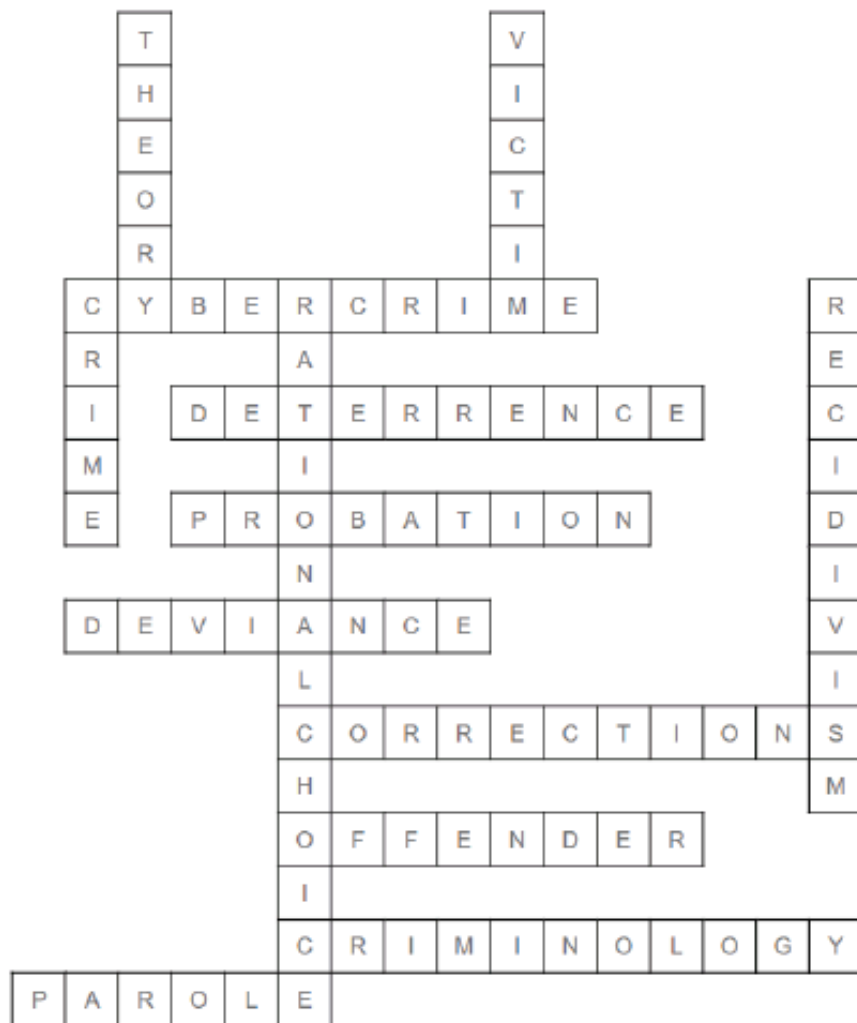
Five tips for cyber-criminology students

-By Nyalock Gatwech

1. Not many people start in cybersecurity. Most of my peers, colleagues and many industry professionals have varied education and professional backgrounds. In my experience, I've found it to be a common sentiment that no one intentionally pursues cybersecurity, with many having 'fallen' into the industry.
2. Studying Criminology enables you to critically assess the intrinsic complexities that similarly exist in cybersecurity. If you are looking to pursue a career in cybersecurity as a Criminology student don't discount an opportunity.
3. Find mentors - Delving into a space you are unfamiliar with in any sense is can be daunting. Building connections with your peers, teaching staff, and mentors will support you in beginning your journey in the industry.
4. Embrace diverse thought and perspective.
5. Seek opportunities - Don't be afraid to reach out to industry professionals, teaching staff or your peers to find out what opportunities there are out there for you.

*Next issue will be
out in July 2024*

crossword answers

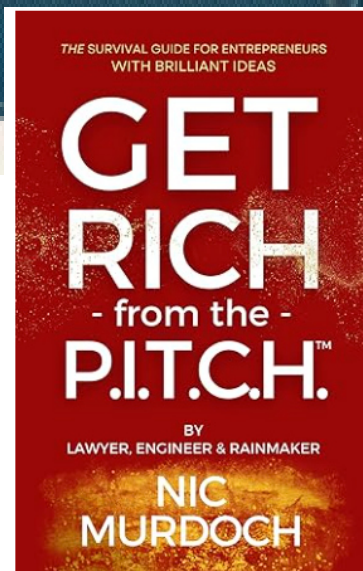


Have you seen these?

Note - this is not sponsored, these are shared to support members of the cybersecurity, privacy, and criminology community.

Nicole is a lawyer, engineer, and a well known presenter at cybersecurity conferences, She is an expert in her field and this book has been a long time coming. It is about how to get your ideas and initiatives past the sketch book scribbles and into something that may make money. Do not be put off by the whole snazzy sparkly cover with the 'rich' word... it is not a scam get rich quick book. If you just want to bring your ideas and creativity into fruition, gift your ideas for the greater good, or just have a heap of projects on the go and want to make something of them for yourself personally and never show the world and never intend to make money from it, this book is still for you as it helps you formulate your plans into something realistic, attainable, and attention grabbing.

Nicole is an expert in her field, she writes well, and is entertaining and informative.



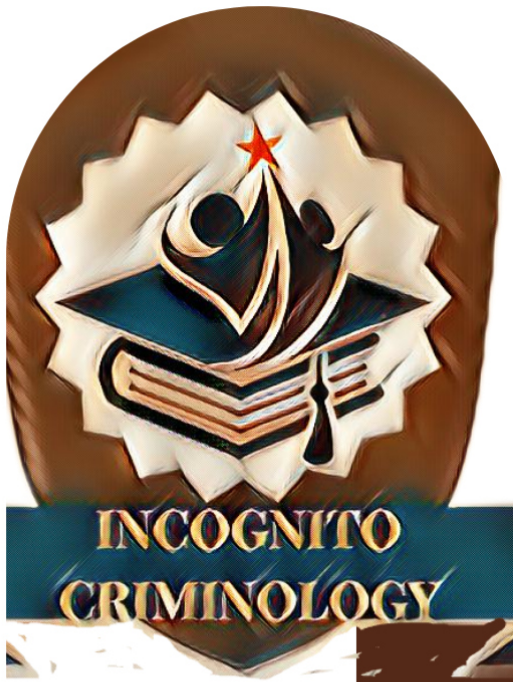
Available
from
Amazon

The Women in Security magazine is the initiative of Abigail Swabey, and part of the Source2Create portfolio. It is free to subscribe to the digital edition, what are you waiting for?

<https://womeninsecuritymagazine.com/>



If you or someone you know would like to be featured in the magazine for free, please let us know, The person or product must have a good reputation and be a part of the cybersecurity/ security/criminology/academic/privacy industry in some way



Magazine

WWW.EMPRESSBAT.COM/MAGAZINE
SUPPORTING CYBER-CRIMINOLOGY
& FUTURE PROOFING THE
CYBERCRIME FIGHTING WORKFORCE
INDEPENDENTLY PUBLISHED

New issue
EVERY TWO MONTHS

About the editor & creator

Amanda-Jane T is a multi-award winning cybersecurity professional - Top 4 in the Global Cybersecurity Influencers for end users in 2022 (IFSEC), keynote speaker, author, mentor, adjunct lecturer in cyber-criminology, and researcher. She is keen to embrace new methods to protect against cybercrime and to future proof a sustainable diverse cybersecurity workforce

IN A WORLD WHERE CYBERCRIME IS RAPIDLY EVOLVING, STAYING AHEAD IS NOT A LUXURY IT'S A NECESSITY. WE NEED TO EMBRACE NEW THEORIES, PRACTICES AND POSSIBILITIES TO ENABLE A FUTURE PROOFED, SUSTAINABLE, CYBERCRIME FIGHTING WORKFORCE.

CREATED &
EDITED BY

AMANDA-JANE T
Cybercrime specialist



email submissions plus your bio to
incognitocriminology@gmail.com

COLLABORATIONS

NYALOK G

Cyber security culture



MIKE HOLM

Cyber security & risk expert



SHAKIRA M

Cybersecurity Intel Analyst



incognitocriminology@gmail.com

www.empressbat.com



[@empressbat](https://www.instagram.com/empressbat)



[@empressbat](https://twitter.com/empressbat)

Submissions Welcome

Anyone who wishes to write a topic relevant to the magazine theme is welcome to submit an article for publication.

You do not need to be an expert or an academic to be given a voice on a relevant topic.

Accepted topics include but are not limited to:

- Advocating for cyber-criminology
- Convergence of criminology, security, and privacy to better mitigate cybercrime
- Applying traditional criminology theories to cybersecurity
- Emerging cybersecurity risks and how to mitigate
- Challenges in investigating cybercrime
- Discussions on relevant news, laws, or emerging technologies as they apply to cybercrime
- Careers for cyber-criminologists
- Cybersecurity awareness and culture initiatives

email submissions plus your bio to
incognitocriminology@gmail.com

🔍 In a world where cybercrime is rapidly evolving, staying ahead is not a luxury it's a necessity. We need to embrace new theories, practices and possibilities to enable a future proofed, sustainable, cybercrime fighting workforce. This free online magazine, "Incognito Criminology" is dedicated to exploring the vital intersection of criminology, privacy, and cybersecurity.

Incognito criminology
Published by www.empressbat.com