

TOP CYBER NEWS MAGAZINE

MAY 2023

CRAIG FORD THE OUTLIER

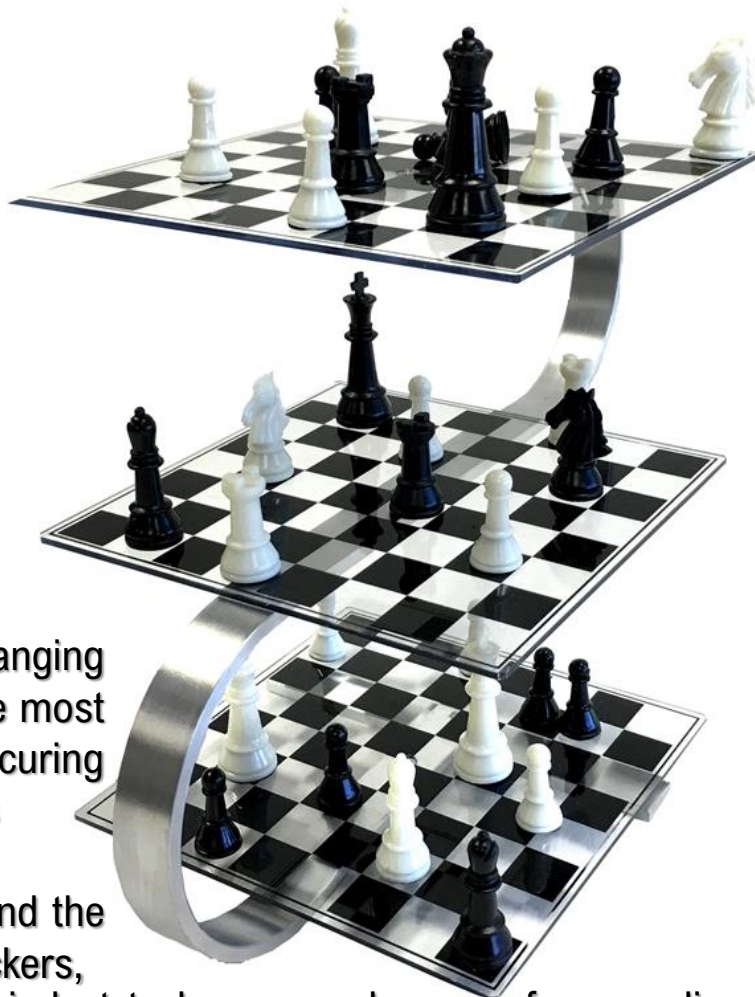
HOW CRAIG FORD, CHIEF TECHNOLOGY OFFICER, ETHICAL HACKER, BEST SELLING AUTHOR IS THROWING AWAY STEREOTYPES AND MAKING CYBER SECURITY ACCESSIBLE FOR EVERYONE. CREATING REAL CHANGE NOT JUST WORDS

Shielding The Defenceless

Finding and Fixing
Vulnerabilities

Safeguarding a
More Secure World

Fore Word



The digital world we live in is ever changing and difficult to keep pace even for the most technical members of our society. Securing it all is even more difficult, which is evident with the ongoing avalanche of cyber breaches happening all around the world. We need to think more like hackers, really get into that malicious actor mindset to have any chance of succeeding with this virtual battle that is starting to spill over into the real world.

Ethical hackers or more specifically hackers need to play a big part in this fight, we need to use their skills and knowledge to help us make the best decisions with the limited resources that we all have available to us. Its better to have a hacker for good, testing your perimeter, your new apps than having your name splashed all over the news when the real criminals knock on those defences.

We all have a place in this war, ethical hackers are knights in this battle, lets embrace them, embrace diversity, embrace the differences in our thoughts across the board and truly start to push back the hordes as they assault our way of life. If we can't embrace this new world with all of our differences than our way of life will fall. **Let's stand tall together, as one.**

Integrating Excellence With The Future!

Top Cyber News MAGAZINE



Do You Have Innovation Blockage?

Editorial by Anthony J James,

CEO, Innovation, Technology & Growth at Trinity Consulting, Australia

Much has been written and present in the technology and business press lately about the notion of 'unlocking' innovation in organisations.

From research organisations to financial news commentators, to Harvard bloggers, the emphasis has always been on finding a means of opening up traditional industries to the benefits of innovation, and to let the natural innovative tendencies of staff to be tapped - a kind of innovation bloodletting. The problem with these perspectives is that there is an assumption that organisations are failing to recognise the need for innovation, or somehow assuming that their staff are not empowered to effect change. It's a patronising critique at the very least, and it misrepresents the barriers to adoption of innovation within both agencies and organisations.

Innovation is not locked up. It's blocked. And for the most part, it's blocked for good reasons, or at least for reasons that are designed to protect the firm.

Innovation is inherently expensive and challenging for large firms. Innovation in business processes, for instance, mean that firms will often need to invest in new technologies or add subscriptions to cloud-based services, and they will need to train staff in use of these tools in order to maximise the value of the investment.

Policies for **data handling** need to be updated, integration of data with recording systems (timesheets, HR management, business analytics) will have to be assessed and intermediary systems implemented where required.

And where staff are either made redundant as a result of business process improvement, or if staff require retraining to take on different duties, executives need to plan for handover and/or redistribution of staff resources with sufficient time and delicacy to implement.

Then there's the risk to the firm for productivity losses during transfer to an innovative process - teething problems - and there are the reputational costs associated with those productivity losses. There may even be legal repercussions for changes in how business data is processed, both between a firm and its customers, and between a firm and its supply chain. Then, process innovation inevitably involves redesign of all dependent systems, and so the speed of transactions and process completion is retarded as new behaviours are learned. Only through repeated behaviours can staff truly maximise the benefits of a process improvement.

And that's just process innovation!

Production, distribution, transaction and communication innovations have another whole series of costs and challenges that render innovation even more expensive and difficult to support. It's not that executives can't see the value of a business innovation. It's not that innovation needs to be unlocked. It's just that the time, productivity, reputation, legal, financial and human resource costs of implementing innovation may exceed the benefits of adoption.

And so innovation is blocked to ensure ongoing production and core business activities (and cash-flow) rather than putting the company at risk.

It is important to understand why these blockages to innovation have been put in place. The challenge is not to unlock innovation but rather to remove the inhibitors to adoption.

That involves a three-pronged change management approach (not without their own challenges):

1. Mapping of business activities within a firm to identify weaknesses in systems and determine dependencies
2. Cultural shift to green light, rather than red light regulation of staff and business activities
3. Project the opportunity costs for failing to support innovation over extended periods of 3-5 years

These three activities have their own costs for firms, but they change both the attitude to innovation in firms, and they improve the understanding of the cost implications of innovation. Only after these have been properly undertaken can an innovation culture be fostered.

Unfortunately, many commentators on innovation in enterprises only get to speak with forward-thinking C-suite executives, and thus their perspective on openness to innovation is skewed.

In The Spirit Of The Times

Chairperson of the Board, Group CEO, Innovation & Growth at **Trinity Consulting Services**, Sydney, New South Wales, Australia, **Anthony J James** is a highly innovative, creative and technology-savvy individual with a passion for continuous learning and a natural talent for leadership, Anthony J James is dedicated to driving positive change and shaping the future through ideas and innovation. With a proven track record of success and a drive to stay ahead of the curve, he is constantly seeking new challenges and opportunities to expand his knowledge and make an impact.

These executives generally understand the value of innovation, and they are open to the idea of distributed R&D, agile methodologies and a customer-experience driven business.

They want to facilitate innovation.

They don't have to unlock innovation; they already know how they want it to happen. It's the **middle management** and **traditional stops** and **checks** on trade that are the blockages to innovation. And they are there to maximise profitability and performance of a firm, while reducing the risk. So until a firm changes the way risk is viewed, how business activity is policed and how the firm will be affected by failing to change, freeing up innovation within the firm won't be a bloodletting, it will be a haemorrhage.

We need to stop considering innovation as a policy, or a hidden attribute of staff and networks that needs to be 'unlocked', and acknowledge that innovation is a product of open business people and processes.

Change the business first. Then innovation can be allowed to flourish.

What does it look like inside your organisation?





DOCTORAL VIRTUAL OPEN HOUSE

Attend a free information session to find out more about Capitol Technology University and our online Doctoral Programs taught by world-wide academics and industry experts with a global perspective.

Small cohorts, responsive professors, and dynamic, experienced peer groups allow doctoral students to imagine and test new boundaries and ultimately become a conduit of new knowledge for others.


Scan the QR code with your mobile device's camera app to access registration page:



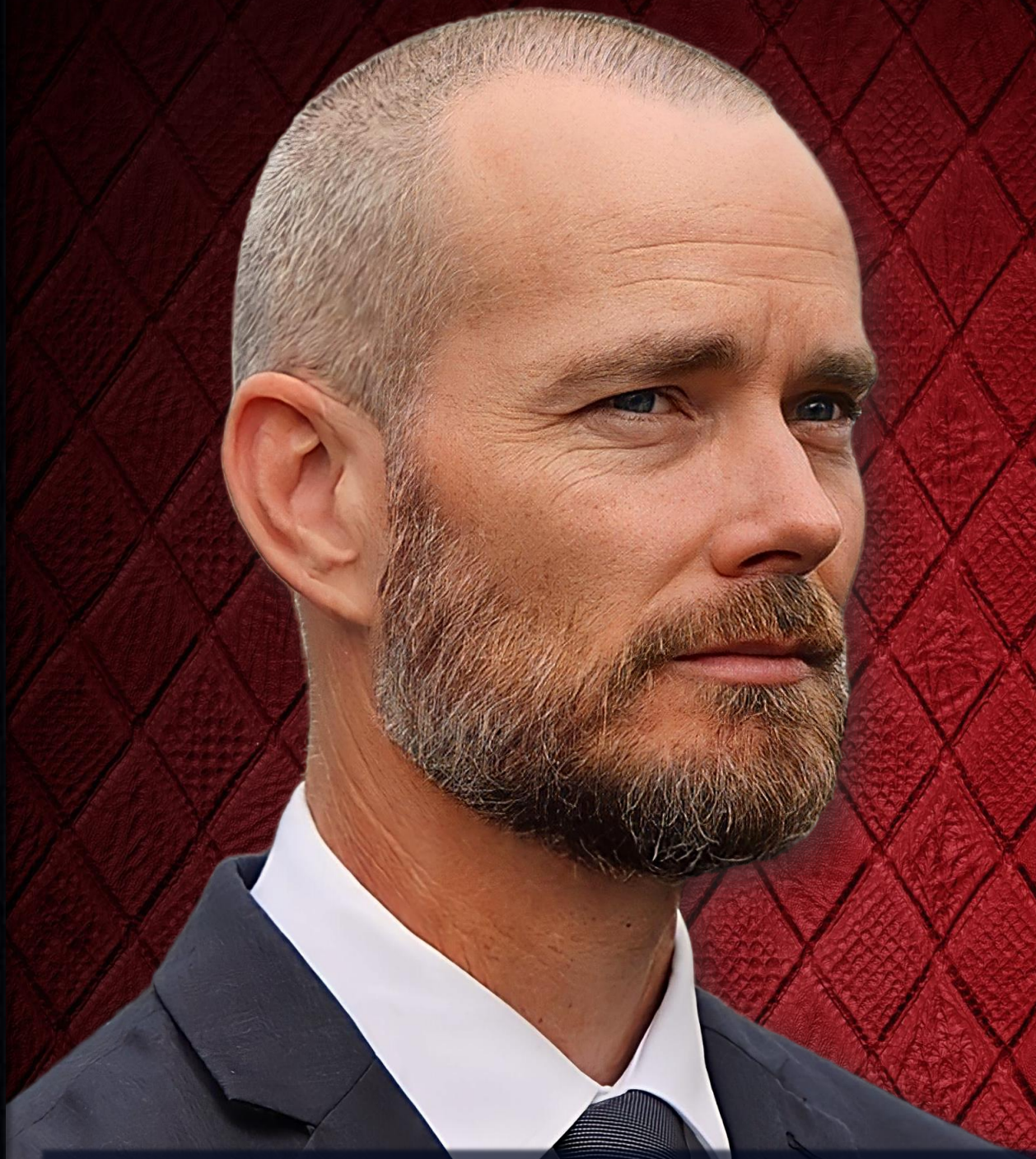
We offer virtual open houses once a month on **Sunday at 3 p.m. ***

2022 Dates	June 11, 2023
November 13, 2022	July 16th, 2023
December 11, 2022	August 13, 2023
2023 Dates	September 10, 2023
January 22, 2023	October 8th, 2023
February 26, 2023	November 12th, 2023
March 19, 2023	December 10th, 2023
April 16, 2023	
May 21, 2023	

* Eastern Time (UTC-05:00)

To register, visit www.captechu.edu/doc-info  doctorate@captechu.edu

Craig Ford, Australia



A cyber security professional with experience working in ethical hacking, incident response, security consulting, **Craig Ford** has two master's level qualifications from Charles Sturt University with a Master of Management (Digital Forensics/Information Technology) and a Master of Information Systems Security. He is proudly employed as the **Chief Technology Officer (CTO)** for **Baidam Solutions**.

A published author with five books - 'A Hacker I Am' and 'A Hacker I Am Vol 2' in his cyber security series and 'Foresight', a Hacker/Cyberpunk novel series that includes Foresight and Shadow books. Vulcan (book 3) is scheduled for release in November 2023. He is also the co-author of The Shadow World, a cyber security awareness book for primary school children.

A freelance cyber security journalist, Craig happily contributes to **Top Cyber News MAGAZINE**. He has a regular column for the "Women in Security" magazine; writes for Cyber Today, Cyber Australia and Careers with STEM magazines. The AISA (Australian Information Security Association) cybersecurity professional of the year 2020, Craig was a member of the AISA Queensland executive team from 2020 until he was appointed a member of the National Board of Directors in January 2023.

Following The Unbeaten Path

by Craig Ford

I am a country boy at heart, having grown up in regional New South Wales Australia, in a place called Inverell. It had less than ten thousand people and was a big central hub for the area, most people knew each other, and I was brought up with what is generally called old-fashioned, country values.



Skippy The Bush Kangaroo! A much loved television show back then! :) C.F.

I started my technology career back in the early 2000's just after the whole millennial bug, which never really made an impact like everyone thought it would. Good for jobs at the time though, bringing in people from all different career backgrounds and skills. We could do with a bit more of that in the cyber security industry today.

My first real tech job was at a local computer store, it was a 12-month traineeship that ignited the beginning of my career. I had always loved technology, I just understood it, TVs, Electronics it didn't matter, given a bit of time I could figure it all out.

I grew from that original traineeship to become the lead technician in the organization travelling a few hundred kilometres in any direction to provide support to clients and build networks and servers. You name it, I would build it and support it. I was a generalist with foot-deep skills across a wide array of tech, but I loved it and stayed in the organization for more than five years. I was always pushing myself to do more, to be better. At around the five-year point though, I found myself in a position where I could not learn anymore, I had reached the level I could achieve, and there was no way up for me. I either stayed and became stagnant or I moved on. I decided to move on and headed to the city to take up a position as the internal IT support for GCT (Gold Coast Tourism), this was my first internal support role and I have to say was a bit of an eye-opener for me.





Not necessarily because of the role itself, yes it pushed me but more about who I was working with.

Russell the CIO was a big influence on me and was a big reason I became so ambitious in my career moving forward. Russell made me believe in myself, and in my ability to be more than just a tech. A thought that had never crossed my mind, I never considered I could become a CTO/CIO/CISO or anything along those lines. I was a country boy who was just good with tech stuff.

I had no formal qualifications and no university degrees. No one in my entire family had finished high school (except me), let alone considered university. I wasn't the perfect student growing up, I didn't enjoy school most of the time, I was just there because I had to be. I wasn't necessarily bad or anything, I just went through the motions, doing the bare minimum to scrape through. I didn't draw attention to myself, I didn't break the rules, just coasted my way through life.

I don't regret not being engaged at school in my younger years though, yes, I could have saved some time, maybe even achieved some of my goals earlier but I wasn't ready to take that path yet, I needed to get out and make some mistakes, get my hands dirty before I could understand what I wanted to do with my life. Sometimes I still don't know the answer to that question so how I am supposed to know at 16 or even 18 years old finishing school? In saying that though I know some very passionate 18-year-olds who know exactly what they want to do in life, their passion is almost a part of them and that is amazing.

I just wasn't one of those people, I took the IT path because I was good at it and it wasn't working security on the door of a bar or at the local shopping supermarket which I had been doing since I left school to pay the bills. Remember, you won't always start out in your dream career or honestly, you may not even like what you need to do to put food on the table but that doesn't mean we can't dream, we can't find new passions that ignite a journey that takes us in a direction that is a little unexpected.

Russell my first CIO, set me on the education path, although I didn't start my CSU degree's (yes more than one) until after I left GCT it was he who made me feel like I could do it like I should strive to be what I was capable of. My first real mentor, without actually knowing at the time that's what he was to me. It's strange isn't it, thinking back on things and realizing the impacts we have on people's lives and the impact that others have on ours.



'BE TRUE TO YOURSELF!'

~ CRAIG FORD

After GCT I returned to Deskline, the small IT shop to run it as the general manager for three years, when the owner Andrew asked me if I would do it I thought it would be a great opportunity to build those management skills. During those three years, I started my first master's degree at Charles Sturt university. This degree was a pivotal moment in my life, one that I was not expecting for a few reasons. For one, it changed my career path completely.

When I started it, I wanted to be like Russell, a CIO, an IT manager but out of complete randomness during the process of signing up for my units, I chose digital forensics and incident response subjects. Just because they sounded cool, seriously that is actually why I did. No desire or big-picture plan here, I just thought they were cool. Crazy right?

I worked my way through some of the required units in my IT management degree and when I finally got to my first unit on digital forensics, I was bitten, I loved it. From that moment I knew exactly what path I wanted to take, and it was not IT management. This was around 2013-2014 and since that time I have never stopped absorbing, always pushing to learn and be better. Security was my career aspiration, yes long term still in a management direction but I was hungry for knowledge and I found my fountain to drink from.

I started to do anything security I could volunteer for, firewalls, antivirus and cyber incidents (although I feel like they were a lot less frequent back then). I continued to do this in my next two positions, just doing security as a part of my normal IT roles. I was learning so much and it was beneficial for my MSP (Managed Service Provider) and enterprise employers.

I even signed up for a second master's degree with CSU in Information Systems Security about a year after I finished the first, I just needed to keep pushing myself, I wanted a full-time career in cyber security, but I didn't want to do it as a part of my job long term, I wanted it to be my job.

It wasn't easy to make the change, I will be honest, it was frustrating and I almost gave up on a few occasions. I had taught myself hacking skills, I had been doing internal testing for my employer at the time and was getting really good at what I did, I had so many knockbacks for positions I almost lost count.

The opportunity did come though but not from a job I applied for, it was via a contact I had made on LinkedIn, an owner of a Brisbane-based MSP who saw my experience in security but also my very well-rounded IT support skills. Exactly what he needed to run security services in his business, I could step in and help with Level three issues and be very useful in times of need as well as give his clients a solid security capability that they were missing until this time.

It was my real starting point in security, I found my niche, my place to thrive. It's a little crazy to think back on what I have achieved since that first day in that role. I am now a member of the board of directors for the Australian Information Security Association, I am the CTO of Baidam Solutions an Indigenous cyber security consultancy firm, I regularly contribute to five cyber security publications as a freelance cyber journalist and I have just started the publishing processes for my sixth book due out in late 2023.



My journey is only just getting started.



CAPITOL

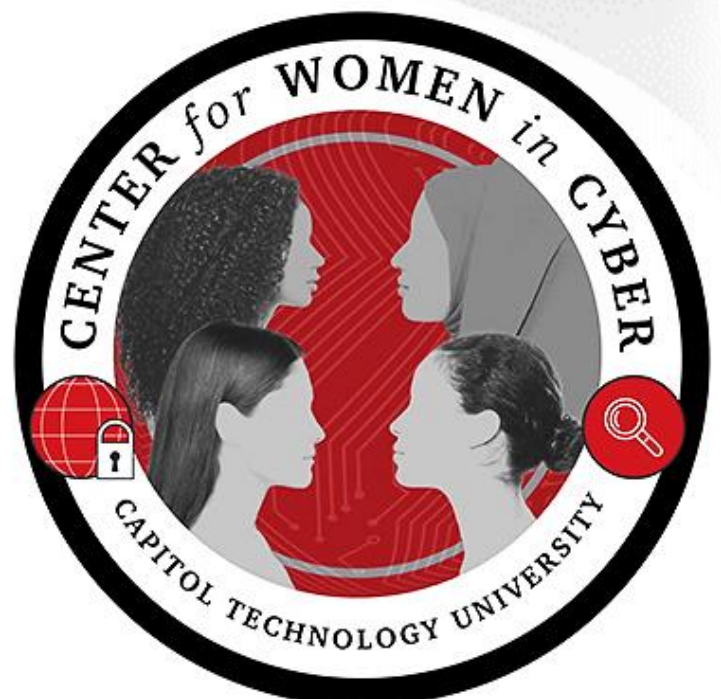
Technology University



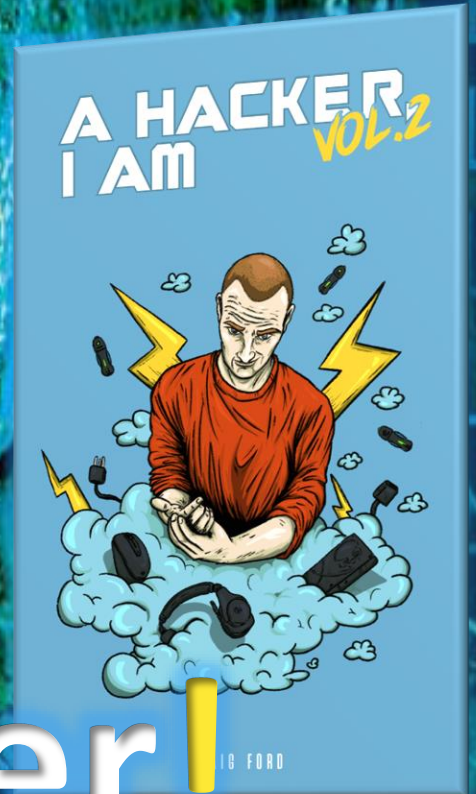
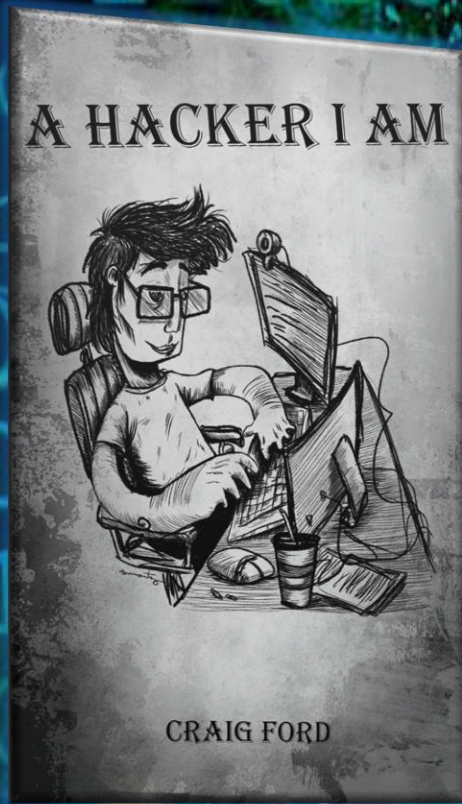
Capitol Tech **Center for Women in Cyber**

Welcome to the Capitol Technology University's Center for Women in Cyber (CWC)! The CWC is focused on empowering women of all ages to pursue careers in cyber. This Center seeks to address the growing need for women professionals and leaders in cyber-related fields.

The Center for Women in Cyber (CWC) will be hosting a virtual Leadership Retreat event for those interested in networking with leaders in cyber and learning more about what the CWC has to offer! This one-day retreat will feature a variety of topics and activities to engage participants with leadership and other members, as well as explore the areas of cyber education, employment, and professional development. Discover all the ways that You Belong in cyber!

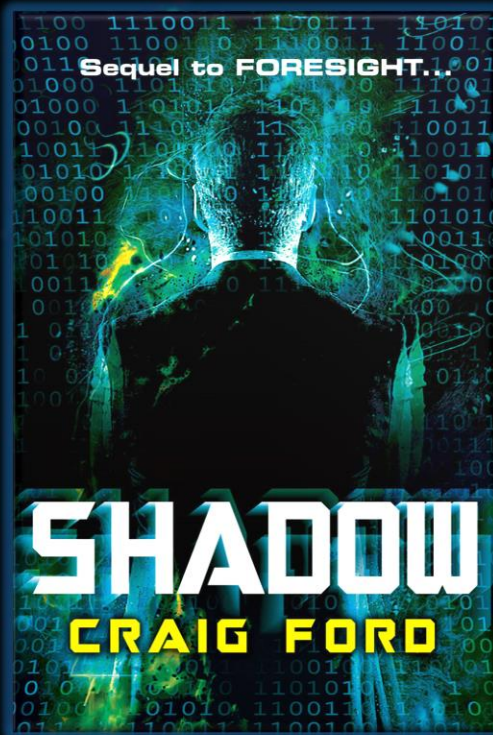
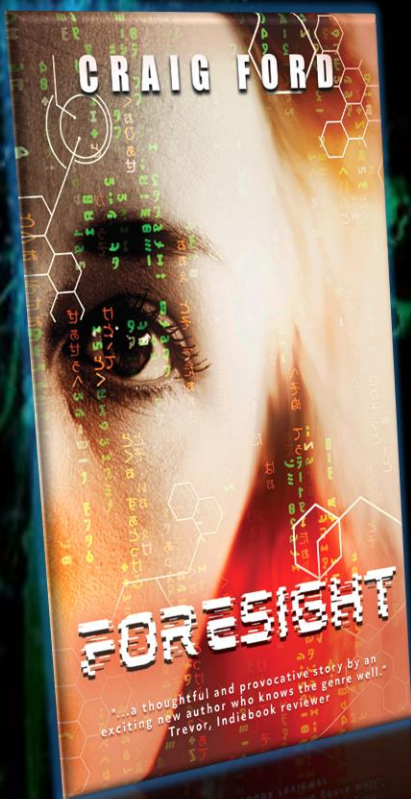


Let's Change The World



Together!

~ CRAIG FORD



Grabbing Onto The Unexpected

by Craig Ford

It is funny how life throws us unexpected curveballs, some good, some bad and some interesting surprises that we could not have imagined. Writing is one of those surprises for me, it was something that I had never considered doing, I was never a book lover as a child or even most of my adult life. I don't have a large book collection like many authors, yes I have a few favourites like the inheritance, rangers apprentice and I am number four series but outside of that, I have mostly educational books that I have collected during my studies over the years.

Writing is one of my passions that truly enriches my life, it gives me an outlet to share my thoughts and ideas. It allows me to escape my reality when desired and allows me to do the same for my readers. I certainly don't follow any traditional writing rule book, I do what feels right.

My writing journey started with what I call a need to share a message, a hidden threat that I didn't feel my industry was talking about and it scared me.

It was 2018, I was attending the last ACSC cyber conference in Canberra Australia, the audience was mostly government and large enterprises. I was working for a Brisbane-based MSP (Managed Service Provider) and had been listening to session, after session all focused on internal defences and malicious actors. The sessions were great and I learnt a lot from peers but the whole time I had this nagging threat that no one was talking about, one I had been thinking about for a while.

MSP's. Yes, that's right the MSP like the organisation I worked for was a bigger threat to most of these organisations that were at the conference and many organisations in Australia and around the world.

They held all the keys to organisations, they had access to almost everything (if they didn't have complete access) and they were essentially unchecked.

If a malicious actor gained access to an account for a senior member of an MSP team they could get access to potentially hundreds of organisations, they could have a smorgasbord, taking whatever they wanted and it could go undetected for months or even years if they wanted it to.

I know, you are sitting there reading this and going. 'What does this have to do with his writing journey?'. Well, it actually has everything to do with it. Let me explain why.

That problem, the lack of discussion brought about a decision that changed my life. It gave me a choice, one I had not considered before. What was that decision? I wanted to raise the issue with MSPs and the risk they posed and have a robust conversation with my peers about how we could fix it or at least make sure we were all aware of it. I needed a platform, a way to give my thoughts and perspective on the issue but the conference was finished.

I had been reading articles from the CSO-Online cyber news site for a few months prior and remembered seeing a comment on the bottom of one of the newsletters "if you have something you want to share or an article you would like to contribute reach out to an email address." Was an article a way to start the conversation, it was worth a shot. I reached out and received a response from someone who I now call a friend, Charlie-Mae. She gave me some guidelines of what they would expect and indicated she would be more than happy to take a look at a potential contribution if I sent something through to her.

It took me a few days to put that first article together, I was a bit nervous about how it would be received, whether it would even be published, would my peers value the contribution. I took the leap and submitted the article.

A few days passed and I received a response. It was a slightly edited version of my piece and a confirmation that it was going to be published on the website. My first article lays bare the risk from MSPs. The start of my writing journey that sparked almost 100 articles for CSO and hundreds more since for publications like Top Cyber News MAGAZINE, Women in Security, Cyber Today, Cyber Australia and more.

It wasn't just articles though it is much more than that now with my sixth book in the works for publication and more. ***Writing has truly become a part of my everyday life, a big part of who I am.***

I am now the proud author of three different book series, two related to cyber education and awareness and a third is a cyberpunk hacker fantasy series.

Each of the series has meaning to me, problems that I wanted to help overcome or solve. Let me break them down individually so you can get the true meaning behind them and a true insight into why they have been brought to life.

A Hacker I Am



The first of my book series, A Hacker I Am is a cyber awareness and an insight into my journey into cyber security. It is a self-published book series that is very different from your normal cyber security books. It was created in a similar style as my cyber security articles, to pull the covers off on some complicated cyber security topics but make them approachable for anyone who wants to learn a little more.

Have you ever read a cyber security book, for university or just for self-education? Most of them are horrible dry books that are the best thing you could ever read to put you to sleep. When I was doing my master's degrees at CSU (Charles Sturt University) I disliked how hard these books were to read. I hated reading them, the content didn't want to stick in my head and was just overloaded with cyber jargon.

Not the best thing for anyone trying to start their journey into cyber or anyone who just wants to learn a bit more to keep themselves safer in this digital world we all live in. I wanted it to be different, I wanted it to be fun. So I created a cyber book that tells stories and teaches lessons as you enjoy the fun adventure.

You don't even need to read it front to back, you can choose any topic in any order and just read it. Then repeat until you have read everything.

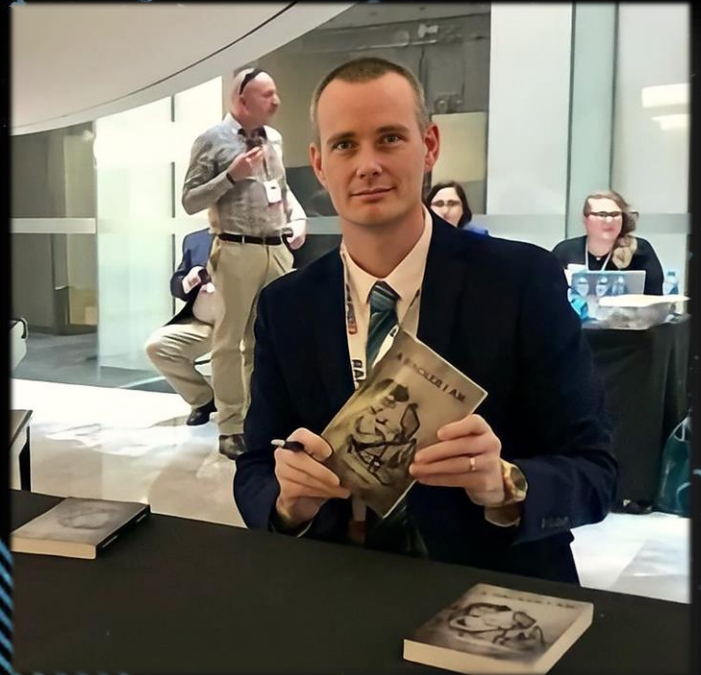
It reminds me of those "choose your adventure" stories, you bought the book, shouldn't you get to choose what you learn first, not be restricted by what order I put them in as the author? It should be fun and engaging, why does cybersecurity need to be dull?



A Hacker

I Am **CRAIG FORD**

During my journey which I share a lot about in the two books in the A Hacker, I Am series I found it difficult to transition from an IT support career over to Cyber, the knockbacks and the roadblocks to gaining entry are painful and is something many people talk about in the industry. We seem to make it difficult for anybody who wants to join us but I honestly don't know why. ***This is why the A Hacker I Am series was created, including the second instalment with A Hacker I Am Vol2.*** I wanted to give new entrants a softer entry into the industry, giving them something that can help anyone get a better insight into problems in the industry and potentially light the spark and entice the reader to look a little deeper.



Foresight Creating a Spark



*Ever since I can remember I have supported diversity and inclusion. I feel the more diverse our backgrounds, sex, and culture the better decisions we can make together. It gives a true ability to look at problems differently and can help to solve some extremely complicated problems. Just because we have done something one way for as long as you can remember that doesn't make it right. **We need to challenge the status quo in security or we will fail it is that simple.***

In Australia female participation in the cybersecurity industry is less than 20%, we as an industry and a country need to do better. I have been a contributor to the Women in Security magazine and the awards in Australia since its inception because I could see a problem but I wanted to do more. How could I, a middle-aged man help improve this?

I have the drive and the passion to help. I decided to create a hacker fantasy series, creating a lead female character called Samantha who was smart, skilled and just a badass, confident woman to give young girls a character to look up to, to read about and go. 'I want to be like her'.

To sit back and think, wow, maybe cyber isn't such a boys club, maybe it's a place for me and my friends to make an amazing career. Let's break the confines of what society thinks or even what industry thinks is normal. Let us forge our way into an amazing industry, not follow the beaten path before us.

Since its release, I have donated almost as many copies as I have sold to as many STEM programs for girls as I could find. The feedback has been amazing, the girls and their parents who read it are loving it but it is not getting into enough girls hands. To truly make a difference it needs to be read by the right audience, to be loved and to create that spark, the one that I found in 2013 when I found myself doing some digital forensics and cyber units.

I knew then and there that cyber was the place for me. I want to create that same feeling, that knowledge that this is their place, where they belong.

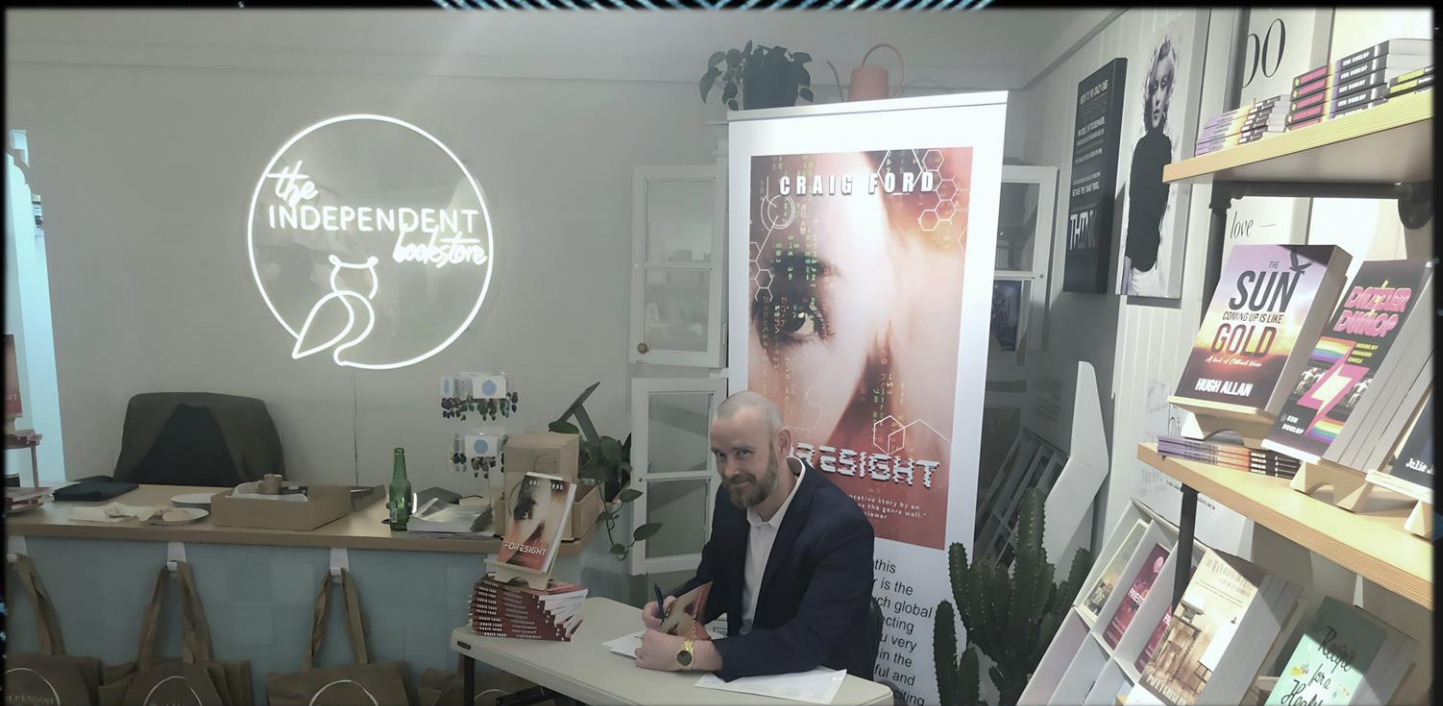
If Foresight can do that for one person, then in my eyes it is successful but imagine what a difference if it could do that for one million young women around the world.

Just think about that for a minute.

Just imagine the difference these amazing young women could make for this virtual battle we are all fighting. Even an additional one hundred thousand young women joining the cyber industry will help tip the balance and help us be better, be smarter in what we do because we will have diversity of thought, an increased workforce getting in and solving the problems that are facing us as an industry or even just society as a whole.

So do us all a favour if you know a teenage girl who you think might benefit from reading Foresight and creating that spark. Give them a copy of the book, make them the new present you give to all teenage girls you know, and help change the industry for the better.

I would do it myself if I could (donate copies to every teenage girl in the world I mean) but I don't have the means to pull off such a feat just yet, so we will need to do it together.





Save the date! August 31st, 2023

@ Ardoe Castle in Aberdeen, Scotland!

A ground breaking event in beautiful Scotland!

Cybersecurity Woman of the Year 2023 Awards Gala Dinner

by Cybersecurity Woman of the Year!

The Inaugural Cybersecurity Woman of the World Edition 2023

by Cybersecurity Woman of the Year, OSP Cyber Academy and Cyber News Global! Organised and announced by Carmen Marsh of the United Cybersecurity Alliance.



CSWY 2023 AWARDS.

NOMINATE NOW!

#CSWY2023



Carmen Marsh, Davis, California, United States

The Importance Of Creating A Point Of Encouragement And Success For Future Generations

I have a lovely memory as 4 years old on the stage reciting a poem for my first International Women's Day in Europe. Some of the details may be fuzzy, but I remember standing on the chair, being so little, barely reaching the microphone. I don't even know if I correctly recited the entire poem, but I vividly remember the tears of women in the front row by the stage, including my mother, and a whole lot of applause. I didn't understand the tears of those women then, but I certainly do now. The younger generations are our hope and dreams of a great future after we are gone.

"We, women, need to continue building the invincible bond amongst us as we bring new generations into the fold, mentor them, and encourage them to take over and do the same when the time comes."

The International Women's Day is here again to remind us of the incredible female power and influence that women had throughout centuries, at different times of our existence; past, present and the future. It is impossible to not be thankful to women from the past who sacrificed so much to fight for our equality and admire those in the present time who are courageously speaking on our behalf about tough subjects, seeking solutions. And certainly, be inspired by young brave girls who are observing, studying, and disagreeing with the current state of humanity.

They are the change makers and instigators of the best version of humanity yet to come.

"It is not only the March 8th, but everyday we can make a difference by being mindfully aware of how powerful, impactful and long lasting our actions can be. I challenge you to step out into the light and become a Starlight!!!"

Definition of "Starlight" – is the grand striking energy of the stars glittering in the night sky that is self-reliant and remind us that we need to be, as well. Starlight has been the big, bold and meaningful guide for many people for thousands of years. Symbolically it tells us to live a life of hope and positivity.

An internationally acclaimed strategist, author, and creative thinker, Founder and President of the United Cybersecurity Alliance (non-profit organization), Carmen Marsh carries out a very important mission and vision to unite the global cybersecurity community as well as provide a platform for women to learn cybersecurity, enhance their skills, and gain hands-on experience for a successful entry and retention within the field.

TOP CYBER NEWS
MAGAZINE
FOUNDERS' SPECIAL EDITION

Carmen MARSH
CYBERSECURITY ROLE MODEL
OF THE YEAR 2021

REALM of CYBERSECURITY
and **INNOVATION**

How Carmen MARSH, President & CEO at United Cybersecurity Alliance, Created a '100 Women in 100 Days Cybersecurity Career FastTrack Program' - to Inspire, Train, Certify, Mentor, & Provide Opportunities for Women in Cybersecurity

The Shadow World

by Craig Ford



I also know what lies beneath the edges of the internet, what hidden dangers await them at every turn, on every app or game they play. The types of people that are waiting to manipulate and extort them at any opportunity. I don't like to be negative but I have seen too much in this space to not be cautious about what activity my kids do.

Some parents allow their children to play games, surf the web and just do whatever they like from a very young age. You see toddlers playing online games on iPads or phones with no supervision or controls. You might say what could a toddler do to get themselves into trouble? Maybe not much, they will not deliberately do anything that could get them in

The online world is where the children of our world live, they communicate, play and they learn all in the digital world. Almost everything is in the digital world, seriously even colouring in is done on an iPad or Tablet in schools. I don't know what is wrong with an old-fashioned pencil and paper.

I would have to say I am a pretty restrictive parent when it comes to online activity and allowing my kids to play games on an iPad or tablet. Considering what I do for a living, I am very anti-tech with my kids. Not because I think technology is bad or anything like that, but because I feel that my kids should learn to interact and live in the real world first before they dive into the digital world.



trouble, they wouldn't understand much about the online world except what they see but if a malicious actor added a link in a chat window, they wouldn't know they shouldn't click on it or even have the thought it would be a danger to them.

A situation like this could still be very damaging and potentially a steep learning curve for the parent. Toddlers though would not be the age group I would have the most concern though, I am thinking between the ages of 6-12 years old. During these years children are starting school and interacting with digital spaces more and more as the years pass by. During the first year of school, they will start to play games, they will get homework via emails and online apps. The older they get the more this will happen.

The concern for me is they are not being taught to be cautious, they are not being taught to consider things are not what they seem, and people are not always who they say they are. Children need to be taught about online danger the same as almost every parent in the world tells their children not to talk to strangers in the real world, this same principle needs to cross over to the digital world. We need sun-safe style campaigns that have worked wonders in Australia created but for a digital world.

Many parents are completely naive to the threats, they have no idea of the dangers that are waiting in the depths. That's why Caity Randall and I created our book *The Shadow World*. It's a cyber security awareness book written for kids between the ages of 8-12 (could be useful for older readers as well or slightly younger if being read with a trusted adult). It uses the concept of shadows and knowledge torches to help the kids reading the book to learn more about the risks and the idea that this knowledge can help light the way through these shadows.

It discusses some serious topics like online grooming, bullying, online gaming, viruses and so much more in 19 chapters. It creates a mindset that it's okay to make mistakes, it's okay to ask for help and not to be ashamed or hide things from the people they trust in the real world. We have even included questions for adults to ask the kids after each chapter, to get conversations flowing between these kids and adults.

We include a thesaurus with any jargon that has been used that will make perfect sense to the kids but may sound like a foreign language to the adults interacting with them. We have created the resource that all parents need in this digital world, a resource for schools around the world to create programs of education around, for libraries to put out on display to help encourage a generational education change, a deeper understanding of the online world and the risk it truly has to us in our daily lives.

By educating this next generation we can all help to push back the avalanche of threats and help create great behaviours before kids grow up and head out to work. Creating true awareness, not an afterthought when it is too late.

That's not all though. Caity and I have been working hard to get this book into as many hands as we can and have already secured a sponsor who will be donating 5,000 copies of this book to primary schools in Australia after its release. Yes, that's right five thousand copies will be donated to schools for free. Imagine this, 5k kids across 50 schools all getting this book for free, they take it home and learn with their parents and maybe even with their teachers in school before they take the book home. This helps educate the kids, the teachers and the parents. Maybe even some of their siblings as well.



We don't want to stop there though, we will be growing this number, really pushing hard to get more books out into the hands of kids for free, and help as many kids as we can to become that little bit more educated online. We will continue to push until every child between the ages of 8-12 has a copy of this book available to them. I don't know how yet but we will make this happen.

If you like the idea and you want to do something like we have done in Australia in your country, find some sponsors and donate as many books as you can to schools, reach out to me, I would love to find a way to get you as many copies as I can at the lowest possible price, I can get you. This isn't about money; this is about education and truly making a difference. If I make nothing from this book but get it into the hands of every child, it will be a success in my eyes.

Let's change the world together, one child at a time.



CRAIG FORD

Baidam SOLUTIONS

Baidam Solutions is an Indigenous owned, Supply Nation Certified Cybersecurity consultancy, with a mission to bridge the gap and create opportunities for First Nations Australians in the IT Sector. We are a for-profit business providing our clients with business-as-usual Cybersecurity outcomes; however, we are focused on delivering a social impact from the commerce we generate. As a by-product of our success, 52% of our profits are directly reinvested into “The Baidam Initiative” to create ICT training and employment pathways for the First Nations community.

Our vision is to bring First Nations people into the ICT industry in a culturally respectful, welcoming and supportive way. By procuring through Baidam Solutions, you help us to deliver role models in the First Nations community, build intergeneration wealth, and support reconciliation through positive employment.

Baidam Solutions is proud to have recently launched the first-of-its-kind co-designed Indigenous owned and run SOC (Security Operations Centre) in Australia to create not only a capable service to clients but to create a safe environment to help train the next generation of security personnel. Helping to generate amazing new talent for the wider industry. We are gifted with one life and we at Baidam will leave lasting change with that life that will be felt for generations to come.

The Darker Side of the Cyber Industry

by Craig Ford

I have been a member of the IT and Cyber industry for around 20 years now. It is a great industry with constant challenges and a never-ending requirement to keep learning. For me that is great I love to push myself and continue to evolve with what my career expects of me. I do the same with my writing, always pushing to be better and to do more. It's just my nature and it can be said for a large percentage of the individuals who work in this space. We are curious creatures who love a challenge (even some we are probably not supposed to – the grey area of ethical hacking), making systems do as they were never intended, defending the undefendable.

Being a part of the industry is certainly not easy. It is said that we as defenders need to get a million things right but attackers only need to get one thing right to get past your defences. That is true and gives merit to the claim that we are fighting an uphill battle when it comes to security. More and more organisations are falling victim to breaches and this is only going to get worse before it will get any better. Of that I am certain.

With this constant bombardment and mounting pressure to keep your organisations safe with probably around half of the required staffing levels, we need. What do you think will happen to all of us?

We crack under the pressures, we start to crumble under the weight. Mental health in this industry is appalling. I have seen it personally on more than one occasion where good people in the industry leave or worse have a mental breakdown because it all becomes too much.

We as an industry need to figure out not only how to get more quality people to bolster our ranks and help relieve the resourcing restraints at least but also need to figure out how to help our people do better with mental health.

We all need to stand up and put our health first. It is after all when you take everything else away what we are left with. If you push yourself too hard and take on too much stress your body and mind will fail you.

This is proven and is happening at an increasing rate. So what can we do?

I am not a healthcare professional but I feel there are some simple things we can do to help us manage our mental states better.


1. Firstly, we need to learn as an industry to put our hand up and say that we are overloaded. We need help. Don't be afraid to ask for some help when you need it, if your organisation treats you badly for asking then that is not an organisation that you should work for.

2. Take time out – disconnect from the chaos that we have to deal with on a day-to-day basis. Get up and refresh from the screens. Too many of us eat at our desks, go outside, get some fresh air and reset. The problems will still be there when we get back. You need to take some of your time. Don't get me wrong, I'm not telling you all to go have two-hour yoga sessions in the park for lunch (you still can if that's your thing and you have that flexibility) but just take a few minutes, take your actual breaks away from **the screens**.

3. Talk to someone – a professional, your friends, your partner, someone if you need to. Don't bottle it up. That won't do you or your organisation any good if you do.

4. If you feel comfortable in doing so, share your experiences with mental health, and let others know that it's okay to talk about it.

These are all simple things but we need to start somewhere. So take a step back and think about what is important. Make changes to ensure you can weather the storm that is inevitable for us all as the digital and real worlds become more and more entwined.



The Power Of The Dyad

Cyberpsychology And Victimology

For The Detection Of Social Engineering Scams

by **Dr. Djalila Rahali**, Cyberpsychologist
Researcher In Cyber Criminality, Algeria

The advent of the digital age has brought about an increase in the number of cybercrimes committed worldwide. Society is becoming more and more technology-dependent and simultaneously more vulnerable to cybercrime. With cybercriminals using advanced techniques to perpetrate their crimes, traditional methods of detecting and preventing such crimes have become insufficient, especially those using social engineering which has become increasingly prevalent in recent years.

These attacks involve the use of psychological manipulation to trick individuals into divulging sensitive information or taking actions that are not in their best interest. Traditional methods of detecting and preventing such attacks have proved to be ineffective. However, the dyad of cyberpsychology and victimology has emerged as a powerful tool in detecting social engineering cyberattacks. This dyad proved to be a game-changer in the fight against cybercrime especially those using social engineering. This paper will explore the power of the dyad in detecting social engineering cyberattacks.

The psychology of social engineering scamming and the causes of its success.

Social engineering scams are designed to manipulate individuals into divulging sensitive information or performing actions that would benefit the attacker. The success of these scams relies heavily on the psychology of human behaviour and decision-making.

Trust is a key psychological factor contributing to the success of social engineering scams. Scammers often exploit the trust that individuals have in certain institutions or authority figures, such as banks, government agencies, or even friends and family members. They may impersonate these entities or individuals to gain access to sensitive information or to persuade the victim to perform an action.

Another important factor is fear. Scammers may create a sense of urgency or exploit the victim's fears to pressure them into taking immediate action. For example, a scammer might impersonate the IRS and threaten the victim with legal consequences if they do not pay a supposed tax debt immediately.

Additionally, scammers often use social proof to make their scams seem more legitimate. They may use fake testimonials or reviews, or create the illusion of popularity by displaying large numbers of followers or likes on social media.

Another key factor is the use of persuasive language and psychological tactics. Scammers may use persuasive language, such as flattery or appeals to emotion, to manipulate the victim into compliance. They may also use social influence tactics, such as reciprocity or authority, to make the victim more likely to comply with their demands. The two are cognitive biases and human has more than three hundred, most of which can be exploitable by cybercriminals.

Overall, social engineering scams are successful because they exploit fundamental aspects of human psychology in a world, I name the “Rertual World” as it is between real and virtual without any limits between the two worlds. Cyberpsychology’s contribution to cybersecurity

Cyberpsychology is the study of how people interact with technology and how technology affects human behaviour. It involves understanding how people think, feels, and behave in online environments. can help to identify the emotions, motivations, and cognitive biases that attackers exploit to manipulate their victims. It is used too, to identify the various personality traits of cyber criminals. This information can be used to create a psychological profile of the cybercriminal, which can help in identifying potential suspects and predicting their next move.

Cyberpsychology can contribute to cybersecurity by:

1. Analyzing users’ behaviour and studying how people use technology so that we can identify patterns that may indicate a potential cyber-attack. For example, if a user suddenly starts accessing sensitive data from an unusual location or at an unusual time, this could be a sign of a security breach.

2. Providing insights into how people behave when they are targeted by cyber attacks. For instance, people tend to make errors in judgment when they are under stress or time pressure, which can make them more susceptible to phishing attacks. Understanding these factors can help cybersecurity professionals design more effective security protocols.
3. Improving awareness by educating users about the risks of cyber attacks and how to protect themselves. This will reduce the likelihood of successful attacks. Example: Teaching users about the importance of strong passwords, how to identify phishing scams, and how to avoid downloading malware.
4. Develop effective training programs for employees on cybersecurity best practices. It is known that training programs that incorporate gamification and simulations can be more effective in improving cybersecurity knowledge and behaviour than traditional training methods.
5. Helping to design more effective security measures. By understanding how users interact with security systems, we can develop systems that are more user-friendly and less likely to be bypassed by cyber criminals. This can involve designing security measures that are tailored to specific user groups, such as employees or customers. In fact, people tend to overlook security warnings if they are presented in a way that is too complex or technical. Designing interfaces that are more user-friendly can help to mitigate this problem.
6. Helping to identify vulnerabilities in human-computer interactions that can be exploited by attackers. For example, people tend to trust computer-generated avatars more than they should, which can be exploited by social engineering attacks

So, by applying the principles of cyberpsychology, we can better understand the psychology behind cyber threats and develop strategies to prevent them.

The contribution of victimology in social engineering cyberattack detection

Victimology plays an important role in detecting social engineering cyberattacks by providing insights into the experiences of victims and the tactics used by attackers. Here are some ways this science helps in detecting cyberattacks:

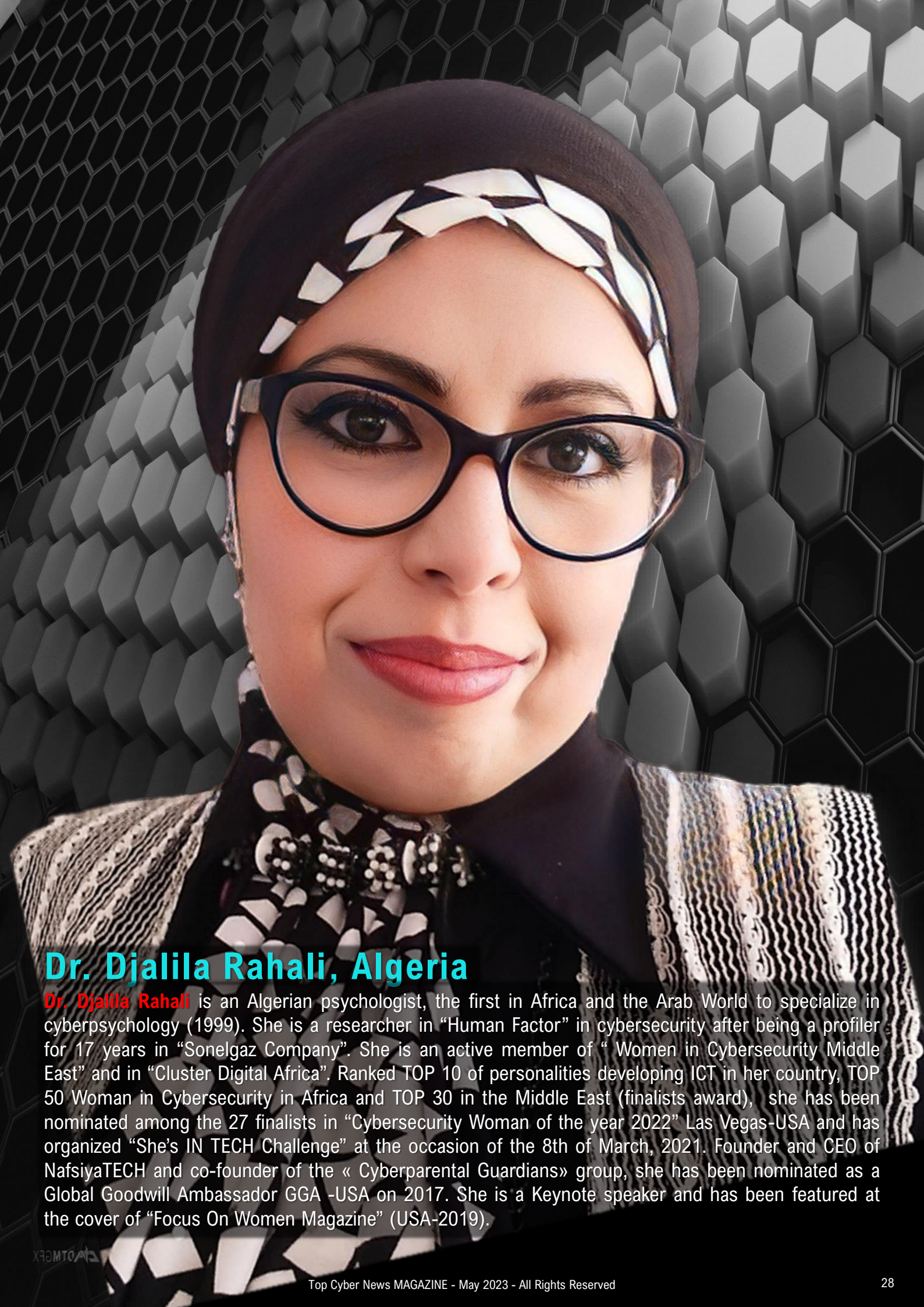
- 1. Identifying common patterns and tactics** by studying the experiences of victims,
- 2. Understanding psychological vulnerabilities** by identifying factors that make individuals more vulnerable to social engineering attacks, such as financial insecurity, loneliness, or a desire for social acceptance
- 3. Providing support, counselling, and informing prevention strategies:** Victims often suffer from psychological distress and other negative consequences. So, victimology can provide insights into the psychological and emotional effects of cybercrime on victims, such as anxiety, depression, and post-traumatic stress disorder (PTSD). This can help cybersecurity professionals develop more effective support services for victims and enhance their recovery. It can also help to encourage victims to report the attack, which can, in turn, lead to the identification of the attacker and the prevention of future attacks.

When cyberpsychology and victimology come together

On social engineering scams, they both can provide a more comprehensive understanding of how and why individuals become victims of cybercrime by investigating the modus operandi of cybercriminals such as persuasion, deception, and trust-building. Victimology research can provide insights into the tactics such as phishing, vishing, and pretexting.

By combining these perspectives, cybersecurity professionals can better understand how social engineering scams work. With the help of computer engineers algorithms using AI can help widely, in the detection of the attempt of scams or cyberattacks.





Dr. Djalila Rahali, Algeria

Dr. Djalila Rahali is an Algerian psychologist, the first in Africa and the Arab World to specialize in cyberpsychology (1999). She is a researcher in “Human Factor” in cybersecurity after being a profiler for 17 years in “Sonelgaz Company”. She is an active member of “Women in Cybersecurity Middle East” and in “Cluster Digital Africa”. Ranked TOP 10 of personalities developing ICT in her country, TOP 50 Woman in Cybersecurity in Africa and TOP 30 in the Middle East (finalists award), she has been nominated among the 27 finalists in “Cybersecurity Woman of the year 2022” Las Vegas-USA and has organized “She’s IN TECH Challenge” at the occasion of the 8th of March, 2021. Founder and CEO of NafsiyaTECH and co-founder of the « Cyberparental Guardians» group, she has been nominated as a Global Goodwill Ambassador GGA -USA on 2017. She is a Keynote speaker and has been featured at the cover of “Focus On Women Magazine” (USA-2019).

Digital World. Behind The Scenes

by **Chris Kubecka, Netherlands**

The digital world brings forward visions of transformation, innovation, efficiency. We are absolutely ingrained in bits and bytes and the convenience they bring. Do you even remember the last time you used a paper map to drive somewhere?

However, behind the scenes is a nefarious game at play. Failures in technology policy and diplomacy plague the industry. The reality of cyber warfare is not entirely new. Previously been clad with a more gigantic body and armed with more powerful weapons than initial strategists ever imaged.

When most people think about the word cyber warfare, visions of exploding items similar to Hollywood movies surfaces most often. However, the reality is much more damaging and insidious.

Focusing on the psychological affects on a population, diminishing trust in government systems whilst turning hearts and minds.

Risks to your Organization and Key takeaways

Proactive Open Source Intelligence against your own organization and key suppliers using tools such as Censys.io or Shodan.io

Start or maintain a robust responsible disclosure policy

Contact and foster a relationship with your national level civilian computer emergency response team

Have an incident management company on retainer

Have an experienced cyber lawyer on retainer

Using her unique technical skills, honed starting age six programming and busted hacking into the DOJ at age 10, **Chris Kubecka** is one of the world's most renown cybersecurity experts.

CEO and Founder of HypaSec NL, COO for LION195 Against Traffickin, former Distinguished Chair for the Middle East Institute's Cyber Program, Chris advises the United Nations, multiple governments, militaries, television and documentary technical advisor as a subject matter expert on cyber warfare national defense.

Author of Hack The World With OSINT Open Source Intelligence Gathering; USAF military combat veteran; former military aircrew, and USAF Space Command, **Chris Kubecka** defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage.

Previous to HypaSec, she reconnected Saudi Aramco international business operations & established digital security after the world's most devastating cyberwarfare attack. Chris lives and breathes IT/IOT/ICS SCADA control systems security.





GLOBAL CYBER CONFERENCE

ZURICH EDITION

SWISS
CISO
AWARDS

PRIORITISING CYBER RESILIENCE

Global Cyber Conference

14-15 September, 2023

Registration is now open

#GCC23



Role of Cyber Security Architect in Securing The Organization

by Dr.K.V.N.Rajesh, India

In today's digital age, cyber threats have become a significant concern for organizations of all sizes. A cyber-attack can cause severe financial, operational, and reputational damage to an organization. Cybersecurity is now a top priority for organizations, and they are investing heavily in building robust cybersecurity defenses. However, ***with the ever-evolving nature of cyber threats, building and maintaining a secure environment can be a challenging task. This is where a cybersecurity architect comes into play. In this article, we will discuss the role of a cybersecurity architect in securing an organization.***

Who is a Cybersecurity Architect?

A cybersecurity architect is a professional who designs and implements security solutions to protect an organization's digital assets. They are responsible for creating an overall security framework that aligns with the organization's business objectives. A cybersecurity architect designs and implements security policies, procedures, and technologies that prevent unauthorized access to an organization's digital assets.

Roles and Responsibilities of a Cybersecurity Architect

A cybersecurity architect has various roles and responsibilities that they need to fulfill to secure an organization's digital assets. Some of the critical roles and responsibilities of a cybersecurity architect are discussed below:

Risk Assessment

A cybersecurity architect must conduct a risk assessment to identify potential vulnerabilities and threats to an organization's digital assets. They analyze the organization's infrastructure, applications, and systems to identify the areas

that are most susceptible to attacks. Based on the risk assessment, a cybersecurity architect designs and implements security controls to mitigate the identified risks.

Design and Implement Security Controls

A cybersecurity architect is responsible for designing and implementing security controls that protect an organization's digital assets. They develop security policies, procedures, and guidelines that align with the organization's business objectives. A cybersecurity architect also implements technologies like firewalls, intrusion detection and prevention systems, and encryption to secure an organization's digital assets.

Security Architecture Design

A cybersecurity architect designs and implements security architecture that aligns with an organization's business objectives. They develop an overall security framework that includes security policies, procedures, and guidelines. A cybersecurity architect also designs and implements a secure network infrastructure that protects an organization's digital assets.

Compliance and Governance

A cybersecurity architect ensures that an organization's security practices comply with regulatory requirements and industry standards. They also develop and implement security policies and procedures that align with the organization's governance framework. A cybersecurity architect also ensures that the security practices align with the organization's risk management strategy.

Incident Response

A cybersecurity architect develops and implements an incident response plan that

outlines the steps to be taken in case of a cyber-attack. They also conduct regular drills and tests to ensure that the incident response plan is effective. A cybersecurity architect also ensures that the incident response plan aligns with the organization's business objectives.

Ethical Hacking

The role of a cybersecurity architect in ethical hacking is to provide guidance and support for the ethical hacking process. The architect is responsible for designing and implementing the security systems and protocols that the ethical hacker will be testing. They must work together to ensure that the security measures in place are sufficient to protect against potential cyber threats.

The cybersecurity architect must understand the vulnerabilities and potential attack vectors that the ethical hacker will be testing for. They must also provide the necessary resources and access to the systems and networks that will be tested. The architect will work closely with the ethical hacker to identify potential vulnerabilities and weaknesses in the system, and to develop strategies to address them.

Performing ethical hacking on LANs (Local Area Networks), WANs (Wide Area Networks), and VPNs (Virtual Private Networks) is an important part of a cybersecurity architect's job. Ethical hacking involves using the same techniques and tools as attackers to identify vulnerabilities and weaknesses in the network infrastructure.

Here are the general steps that a cybersecurity architect may follow when performing ethical hacking on LANs, WANs, and VPNs:

Planning:

The cybersecurity architect will start by defining the scope of the ethical hacking exercise, identifying the systems and devices that will be tested, and setting the goals and objectives of the exercise.

Reconnaissance:

This involves gathering information about the

target network, such as IP addresses, open ports, and network services. This information can be obtained using tools such as Nmap or Netcat.

Vulnerability Scanning:

Using vulnerability scanning tools such as Nessus or OpenVAS, the cybersecurity architect will scan the network for vulnerabilities and weaknesses in the target systems and devices.

Exploitation:

Once vulnerabilities are identified, the cybersecurity architect will attempt to exploit them to gain access to the target systems or devices. This can involve using tools such as Metasploit or Burp Suite.

Post-Exploitation:

After gaining access, the cybersecurity architect will assess the level of access they have, and attempt to escalate privileges or move laterally within the network to gather more information or gain access to additional systems or devices.

Reporting:

Finally, the cybersecurity architect will document their findings, including any vulnerabilities that were identified, the methods used to exploit them, and recommendations for remediation.

It's important to note that ethical hacking must always be performed with the appropriate permissions and in a controlled environment. Unauthorized hacking or unauthorized access to systems or devices is illegal and unethical. Ethical hacking should only be performed as part of a comprehensive security testing plan with proper authorization and oversight.

Overall, the cybersecurity architect plays a critical role in the ethical hacking process by providing the necessary infrastructure, guidance, and expertise to support the work of the ethical hacker. By working together, they can identify and address potential security risks and help to ensure that the organization's systems and data are protected against cyber threats.

SWARM Cybersecurity

In reference to January 2023 edition of Top Cyber News MAGAZINE, where Stéphane Nappo, Vice President, Cybersecurity Director & Global Chief Information Security Officer at Groupe SEB speaks about the moment and the right time for innovative approach towards cybersecurity. The time to take a proactive stance – to swarm cybersecurity - rather than waiting for swarms cyber attacks.

The role of a cybersecurity architect in implementing swarm cybersecurity is crucial. A cybersecurity architect is responsible for designing, implementing, and maintaining an organization's cybersecurity systems and strategies. When it comes to implementing swarm cybersecurity, the cybersecurity architect is responsible for ensuring that the swarm system is designed and implemented in a way that aligns with the organization's overall cybersecurity goals and objectives.

The cybersecurity architect will work closely with the swarm system developers to design and implement the system architecture, including the different agents and their roles within the system. They will also be responsible for identifying and integrating the different security mechanisms required to ensure the security of the swarm system, such as access controls, encryption, and authentication mechanisms.

Another important role of the cybersecurity architect in implementing swarm cybersecurity is to ensure that the system is compliant with relevant cybersecurity standards and regulations. This includes ensuring that the swarm system is designed and implemented in a way that complies with industry standards, such as the NIST Cybersecurity Framework or ISO 27001.

The cybersecurity architect is also responsible for developing and implementing policies and procedures for managing the swarm system.

This includes defining roles and responsibilities for different members of the swarm system and developing procedures for monitoring and managing the system's performance and security.

The Benefits of Having a Cybersecurity Architect

A cybersecurity architect plays a critical role in securing an organization's digital assets. The benefits of having a cybersecurity architect are discussed below:

Better Risk Management

A cybersecurity architect conducts a risk assessment and identifies potential vulnerabilities and threats to an organization's digital assets. Based on the risk assessment, they design and implement security controls that mitigate the identified risks. This helps an organization to manage its risks effectively.

Robust Security Framework

A cybersecurity architect designs and implements an overall security framework that aligns with an organization's business objectives. This ensures that an organization's security practices are aligned with its business objectives.

Regulatory Compliance

A cybersecurity architect ensures that an organization's security practices comply with regulatory requirements and industry standards. This helps an organization to avoid regulatory penalties and reputational damage.

Effective Incident Response

A cybersecurity architect develops and implements an incident response plan that outlines the steps to be taken in case of a cyber-attack. This helps an organization to respond effectively to a cyber-attack and minimize the damage.

In conclusion, the role of a cybersecurity architect is critical in securing an organization's digital assets.

A professional portrait of Dr. K.V.N. Rajesh, a man with dark hair, wearing a blue suit, white shirt, and blue tie. He is smiling slightly and looking directly at the camera. The background is a dark blue with a yellow curved line on the right side.

Dr.K.V.N.Rajesh, India

Dr.K.V.N.Rajesh is a highly qualified and certified Microsoft Trainer who currently serves as a Subject Matter Expert at CloudThat. His expertise is centered around various aspects of Azure Security, including Identity & Access Management, Information Protection, Microsoft 365 admin center, Defender Suite, Microsoft Cloud App Security, and other security operations.

With his extensive hands-on experience in these areas, he specializes in providing tailored training to meet the unique needs of clients and organizations in technical training settings such as Corporate, Online, and Classroom environments. He is truly passionate about technology and continuously keeps up with the latest trends in the industry, as evidenced by his demonstrated skill set in Microsoft 365 Security, Azure AI, and Deep Learning.

With over 18 years of experience in training, he has imparted his knowledge and skills to over 10,000 participants in his career. He holds both a B.Tech and M.Tech in Computer Science and has completed his Ph.D in the area of Deep Learning, highlighting his advanced expertise in the field of technology. His passion for technology and training is evident in his impressive track record and dedication to providing top-quality education to his clients and students. He has been recognized with numerous awards, one of which includes winning the Microsoft Blogathon in 2022.

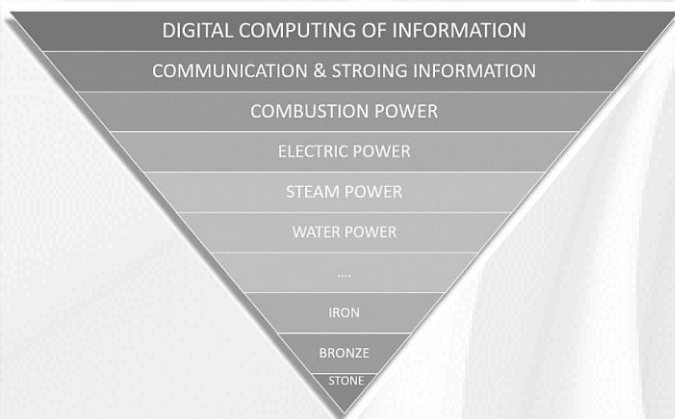
Creation Of Resilience. Together!

Call for Action by Henrik Parkkinen, Sweden

Our world is going through an evolutionary transformation. Societies, humans, and organizations have grown into a new substrate. Digital. The transformation is irreversible, the pace is faster than ever, and we are just at the beginning of this era. The pace will get even faster.

One of the reasons behind this prediction is that IoT, machine learning, quantum computing, AI, and other emerging technologies are still only in their early evolutionary cycles. The real power of these capabilities and technologies is far from fully realized.

Progress in development and advancement are made every day. And the digital evolution, from a macro perspective, is still also in its early phases. This is just the beginning.



The digital substrate has enabled and provided our world with totally new forms and opportunities.

For example, how we as individuals and organizations are communicating, interacting, integrating, exchanging data/information, and so forth. We are more connected than ever before and interrelated to each other. We are living in an amazing era where technology is a true value-adding asset in many different shapes and forms.

And without getting too philosophical we are, according to my personal opinion, already interacting and manifesting ourselves partly as cyborgs. It may sound like hippie sh*t but think about it for a second.

Daily life, for many of us humans, is in one way or another strongly related to and dependent on devices and technologies that enhance our everyday life.

And many everyday life activities have moved into our devices, e.g. smartphones. The smartphone can today be seen as a digital manifestation of our physical selves or as a digital extension. And there will be more to come when technologies such as virtual reality (VR), augmented reality (AR), mixed reality (MR), and extended reality (XR) become more and more mature. And if we just think about the loss of a smartphone/smart device is something totally different today compared to losing a mobile phone 10-20 years back in time. And I also think that losing a smartphone today compared to an extrapolation of 10-20 years into the future will also be something different.

At the moment we are still only in the beginnings of this adventure, the digital substrate. The world we live in today is fascinating in so many ways!

Technology has for example enabled certain kinds of surgeries can be conducted remotely. Cities can use smart technologies to optimize resources. Cars and trucks can drive themselves. Global environmental sustainability can be improved with the help of AI. Technology is used in schools to enhance and improve learning for our younger generations. Education and knowledge are shared more than ever before. These are just a few examples that we almost take for granted right now.



But we shall also be aware of that this is not applicable to everyone living on our planet. All countries and societies do not have the same digital penetration, e.g. internet connectivity, infrastructure, communication coverage, knowledge, skills, etc.

The Asymmetric Landscape Of Security

Part of this evolutionary transformation and the opportunities it provides us with has also generated problematic and challenging scenarios. One of the fastest growing problems for our world is the explosion of cyber security threats and attacks. As digitalization grows into more and more horizontal and verticals, within our organizations and in society, cyber threats and attacks are today a true problem affecting us as humans.

Critical infrastructure such as example, but not limited to, power plants, water pipelines, air traffic, hospitals, and medical devices are today many times connected to the internet. Critical infrastructure is today considered as highly valuable assets, by adversarial threat actors, due to (for example) the amplified negative impact cyber-attacks can cause on us as humans, on society, or on monetary effects on private organizations.

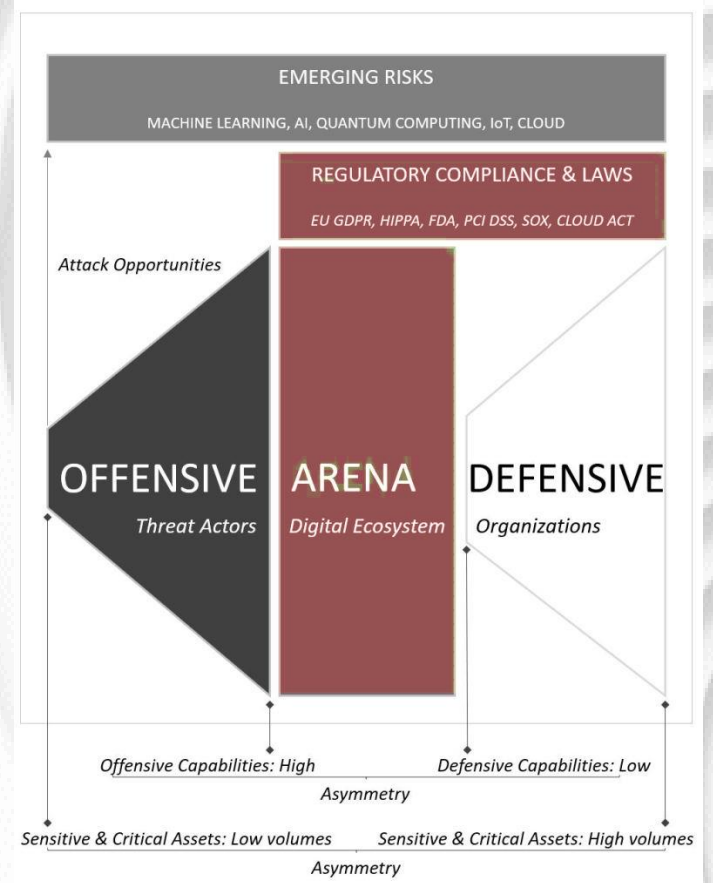
We together need to help each other to develop sustainable and resilient defensive cyber security capabilities. Cyber security is not a one-man show.

In this blog, I will, from time to time, fall back on the wording “resilience”. There are many different descriptions out there of this word of what it means, and I will not argue against those. I am totally fine with that other look at resilience as something else or put another meaning into it. I see resilience as and will refer to the word as:

“Resilience is the product of the capabilities for how an organization or individual is prepared for any form of disturbing or harmful event and from that able return to an operational state.”

So why is resilience important and should be a highly prioritized subject in cyber security?

The digital ecosystem and cyber security landscape are highly asymmetric, the scales are very unevenly balanced between those who carry out the attacks comparison to those defending against the attacks. Many societies



Many societies and organizations are today struggling with keeping up the pace with digital enablement (e.g., realizing value to their organizations through digital capabilities) and at the same time protecting their assets (humans, intellectual properties, IT-landscape, patents, monetary assets, brands etcetera). Defending organizations have to defend against every kind of attack, while the attackers just need to identify one weakness to exploit.

Cyber security, as I see it, is not a discipline that shall be treated, concentrated, or focused only on technology. To achieve adequate protection an organization, need to understand its current cyber security posture and maturity from three perspectives: Humans, Processes, and Technologies.

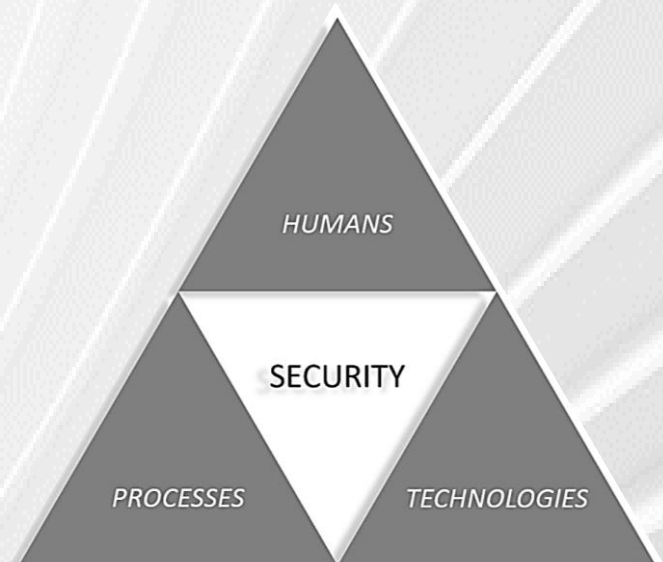
Security Is About Humans, Processes & Technologies

An organization's defensive cyber security capabilities need to be adequately balanced between all three perspectives in relation to the organizational cyber security requirements. The term "adequately balanced" for me means that an organization needs to craft its cyber security posture according to its cyber security requirements.

An organization's cybersecurity requirements are dependent on for example industry, culture, market, history, internal/external security compliance, regulations, laws, asset (e.g. humans, intellectual properties, patents, business information, and data), threats, vulnerabilities, risks (+ tolerance, capacity, appetite). There is no silver bullet, no one size fits all solution.

The solution needs to be adapted and built around three fundamentals: *Humans, Processes, and Technologies.*

And the capabilities need to be continually managed and improved to reduce potential weaknesses and vulnerabilities.



I believe that we together, due to the fact that cyber security is something involving and concern for everyone, need to help each other to achieve a more resilient digital ecosystem against cyber security threats and attacks. There are so much information, knowledge, experiences, and wisdom available to be shared. This blog is my way for how I try to contribute to making the digital ecosystem and cyber security landscape a safer place.

The digital transformation will not solve down, it is here to stay and will only reach a higher penetration rate and pace.

The creation of protection that is sustainable and resilient over time for our organizations and society needs to follow the digital transformation and evolution. And we need to start now and by doing so I think it is best to start from where we are.

Besides those threats and attacks that we are facing right now, there is a strong need of starting discussions around emerging risks related to cyber security. Personally, I think that this was something that was missed out on when it came to cloud services. Many organizations dived head-in-first without contemplating the risks. I truly believe in digital enablement, through the cloud or on-prem services, but investments need to be calculated and assessed from a risk and reward perspective.

This does not only mean a business case needs to be developed rationalizing the monetary investments, but also that a sound risk assessment from a cyber security perspective needs to be conducted.

I think that the primary success factor for achieving this without a negative experience from a business perspective is to educate the involved stakeholders about “why” this exercise is important. And of course, don’t make things more complicated than needed. Keep things pragmatic and in relation to the value of the assets that are to be protected. Every asset in an organization is not as equally important from a business / regulatory / jurisdictional / etc. perspective and for this reason, all the assets do not need the same type of protective measures. **There are several ways how to find out and identify which assets are most important and this is a topic of its own so I will leave you with this cliffhanger for now.**

Doing the work TOGETHER!

Does your organization have a clear understanding of which assets are categorized as the most important for you? If yes, have for example an impact analysis or risk assessment been conducted to assess if those assets are damaged/harmed due to a negative impact from a confidentiality, integrity, availability, traceability, or regulatory perspective?

“Defending organizations have to defend against every kind of attack, while the attackers just need to identify one weakness to exploit.”

Start where you are. Start now. Help each other. Communicate. Educate. Lead and be led. Strive for increased resilience. Together. Henrik Parkkinen, Sweden

Henrik Parkkinen is a security professional from Sweden with +20 years of career experience. He holds several highly ranked industry credentials, e.g. CISM, CRISC, CISA, CCSK. Henrik has a broad and deep understanding of today’s digital ecosystem, emerging technologies, security universe, and threat landscape. The knowledge he holds is a product of experience collected from both a defensive and offensive security perspective through technical hands-on assignments to management and leadership roles.

Henrik has experience from medium sized organizations to international enterprises spanning over the globe within multiple different industry verticals. He also shares his experience and knowledge through his website, www.HenrikParkkinen.com.




100 CISO FORUM

SUMMIT & AWARDS

UAE 2023

Integrating Excellence With The Future!

 Save the date! 19th July, 2023 @ The H Dubai, UAE

We are pleased to announce that Top Cyber News MAGAZINE has been selected as the media partner for the 100 CISO FORUM | Summit & Awards, UAE 2023 by the 3novex Global.

The 100 CISO Forum, Summit & Awards, UAE 2023 has been specifically designed for the Chief Information Officers and Chief Technology Officers, expecting 100 CISOs to be present. Featuring international and local speakers, the forum provides in-depth details and solutions to improve the cybersecurity and information security landscape in the United Arab Emirates. It is a one day summit with interactive sessions, panel discussions, fireside chat, pecha kuchas and more.

TOP CYBER NEWS MAGAZINE

WALL OF FAME 2023



AN AWARD-WINNING DIGITAL MAGAZINE
ABOUT PEOPLE, BY PEOPLE, FOR PEOPLE