Cybersecurity Trends

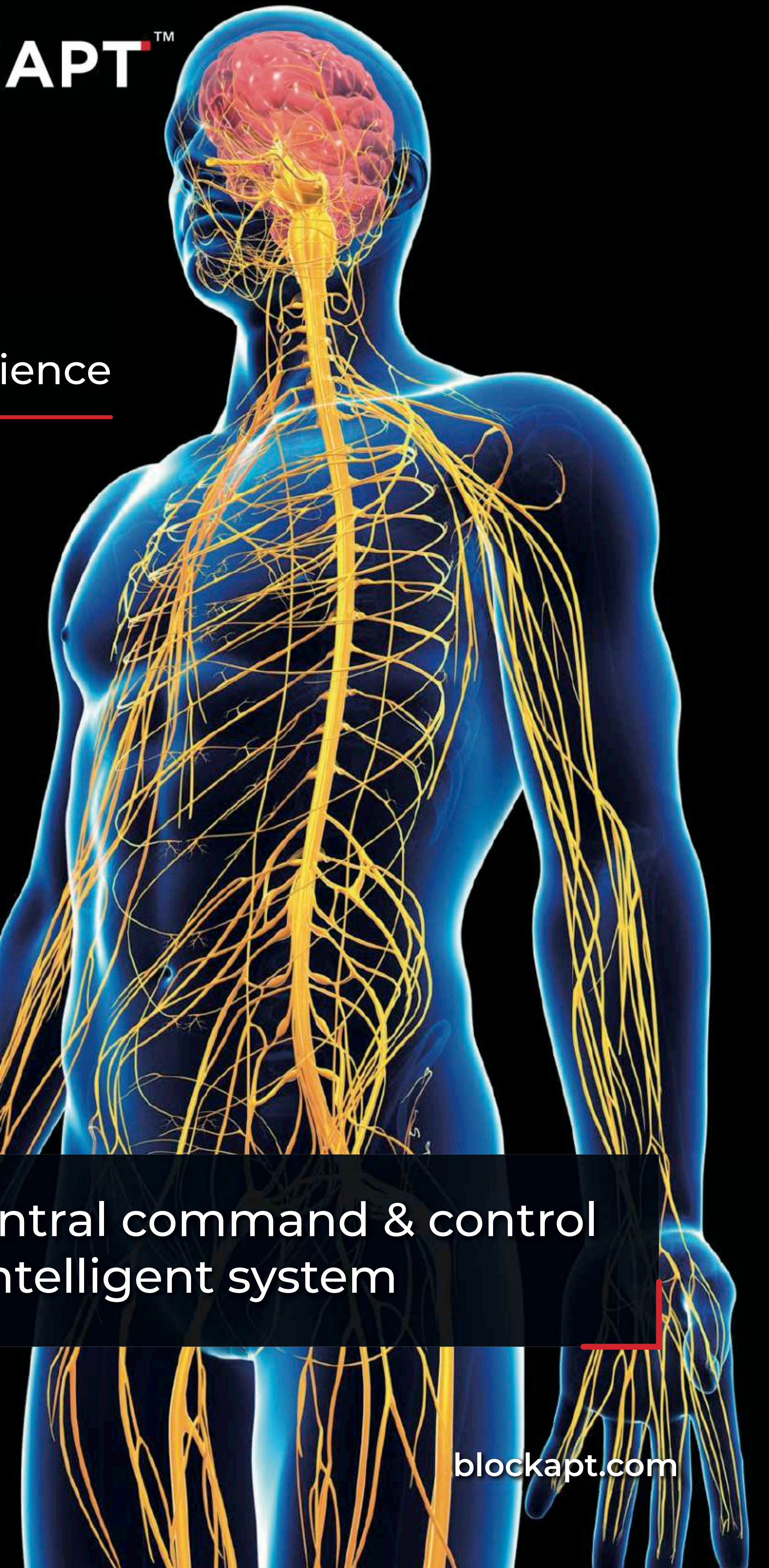
UK edition n.4 / 2022

A Hacker's world... Don't be a Victim... and much more...

See yourself in CYBER

National Cybersecurity Awareness Month

BLOCKAPT™



Single unified platform experience

Digital central command & control intelligent system

blockapt.com

Contents

EDITORIAL

A HACKERS WORLD: HOW THEY THINK AND BEHAVE

DON'T BE A VICTIM: BE SAFE

SEE YOURSELF IN CYBER: A WORLD OF OPPORTUNITIES AND INSIGHT

It's all about the PEOPLE.

Authors: Raj Meghani, Marco Essomba, Laurent Chrzanovski

National Cybersecurity Awareness Month is upon us this October and almost gone but that doesn't mean the show doesn't go on. We have been very active in searching out industry peers and associates to bring you the latest from the world of cybersecurity. In this issue – See yourself in Cyber – we are raising awareness of all thing's cybersecurity with best practice tips.

CYBERSECURITY AWARENESS MONTH

Our aim is to strive deeper into the world of the hackers and understand how they are getting quicker, smarter and more sophisticated with their attacks. We also flip the coin and look at what it is like to be a victim and provide useful guidance on how unsuspecting victims can better protect themselves.

Last but not least, we look at working in the world of cyber – a much needed conversation as we flag the ever pressing need to invest in our upcoming generations to hold the cybersecurity fort in the years to come and help address the skills shortage.

For those who operate as businesses, we share with you thought provoking insights into what you can do to increase operational resiliency and mitigate your exposure to risk. Collaboration, visibility, control and embedding cybersecurity deep into the DNA and culture of businesses are front of mind.

For those who are individuals, we share with you easy to understand hints and tips on ways to protect yourself – this doesn't necessarily mean additional cost. It's surprising how many of the in-built security features in software solutions are not utilised at all.

For those who are looking to enter the world of cybersecurity. A big welcome. It's one of the most rewarding, motivating, fast moving, exciting yet challenging industries you'll ever work in. We hope our contributors' words of wisdom gives you a flavour of the world we live and breathe. Passionately. If you truly put your mind to what you want to do, then you will succeed.

So, we hope these articles inspire you to watch out for the hackers, protect yourself from being a victim and for those still looking to embark on their career path or looking for a career change, give you plenty of food for thought as you explore the riches to be had working in cybersecurity and the many ways in which you'll help make a positive difference to keeping our world secure.

Happy reading! ■

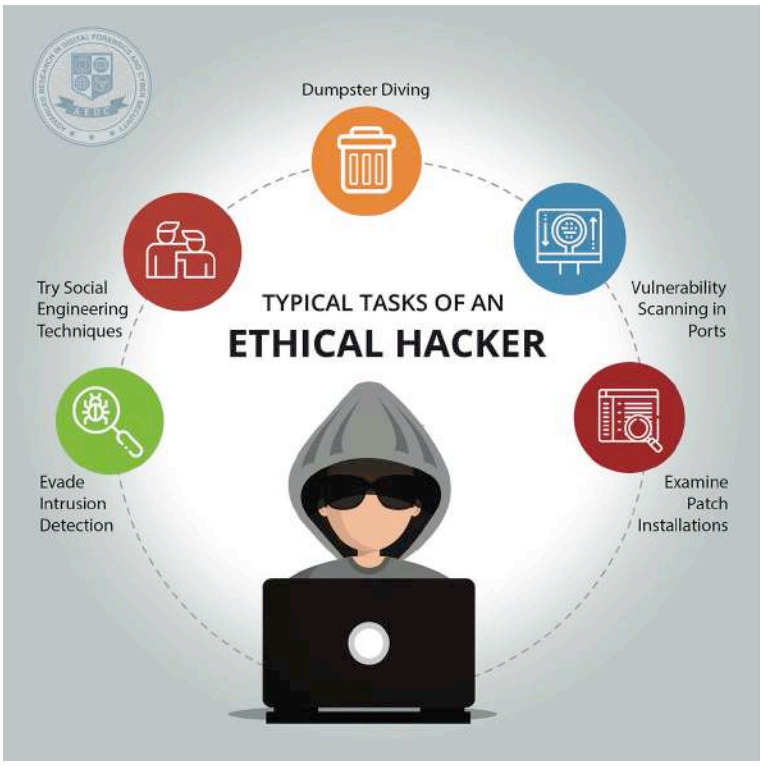
A Hackers World: How they think and behave

How to become an Ethical Hacker & how hackers choose their victims!

Author: Aniket Vilas Chavan

The word **"hacker"** originally defined a skilled programmer proficient in machine code and computer operating systems. Today, a **"hacker"** is a person who consistently engages in hacking activities and has accepted hacking as a lifestyle and philosophy of their choice. Hacking is the practice of modifying the features of a system, to accomplish a goal outside of the creator's original purpose.

What is Ethical Hacking?


TYPICAL TASKS OF AN
ETHICAL HACKER
Dumpster Diving
Vulnerability Scanning in Ports
Examine Patch Installations
Evade Intrusion Detection
Try Social Engineering Techniques

The term **"hacking"** has very negative connotations, but that's only until the role of an ethical hacker is fully understood. Ethical hackers are the good guys of the hacking world, the ones who wear the **"white hat".** So, what does the role of an ethical hacker entail? Instead of using their advanced computer knowledge for nefarious activities, ethical hackers identify weaknesses in data computer security for business and organisations across the globe, to protect them from hackers with less honest motives.

BIO

Aniket is currently working as a Cyber Incident Handler at Atos Paladion. He also specialises as a Threat Hunter and is a Certified Ethical Hacker. In Aniket's spare time, he is active in Bug Bounty Hunting. Aniket is also the Founder and Organiser of Flutter Mumbai and Flutter India.

What is the attraction of an Ethical Hacking career?

If you're a professional who appreciates the joys of the world of computers and relishes a challenge, then a career in ethical hacking can be an enticing prospect.

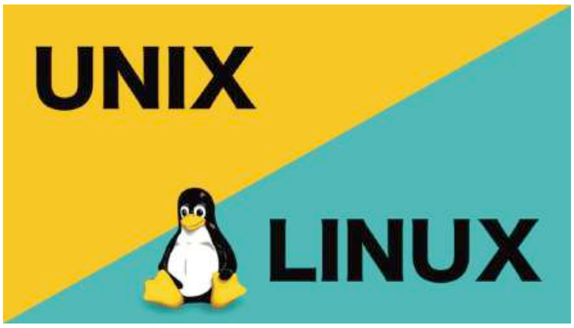
You get the opportunity to use your skills to break into computer systems, and you get paid good money for doing so.

Like many careers, it is not easy to get started in the field, but if you put in the effort, initially, you will be able to shape a very lucrative career for yourself. Besides, ethical hackers are always on the right side of the law!

10 Steps to become an Ethical Hacker

Step 1: Get hands-on LINUX/UNIX

The open-source operating system — LINUX/UNIX, ensures better security for computer systems. As an ethical hacker, you should be well-versed with LINUX as it is one of the widely used operating systems for hacking. It provides ample tools for hackers. Some common Linux distributions include **Red Hat Linux, Ubuntu, Kali Linux, Backtrack,** and more. Among these, Kali Linux is the most popular Linux system specially customised for the purpose of hacking.



Step 2: Opt for the mother of all programming languages

One of the most primitive programming languages, C is also referred to as the mother of all programming languages. This programming language forms the base of learning UNIX/LINUX because this operating system is written completely in C. So, hackers must master C programming as it gives them the power to utilise the open-source operating system Linux the way they desire.

Try to learn more than one programming language to get the upper hand. An ethical hacker with sound knowledge of two to three programming languages can dissect and analyse a piece of code. Some of the best programming languages for hackers are:

- Python: Extensively used for exploit writing
- JavaScript: Suitable for hacking web applications
- PHP: Helps fight against malicious attackers
- SQL: Best for hacking large databases

Step 3: Learn the art of being anonymous

The most important step for ethical hacking is to learn how to be anonymous and hide your identity online so that there is no trace left and none can backtrack you. Often an ethical hacker might not know who else is in the same network, and if a Black hat hacker figures out that there is someone else in the network, they might try to hack their system. Thus, anonymity is vital for ethical hackers as well. Using Anon surf, Proxy chains, and MacChanger are the three most promising ways to safeguard your identity.

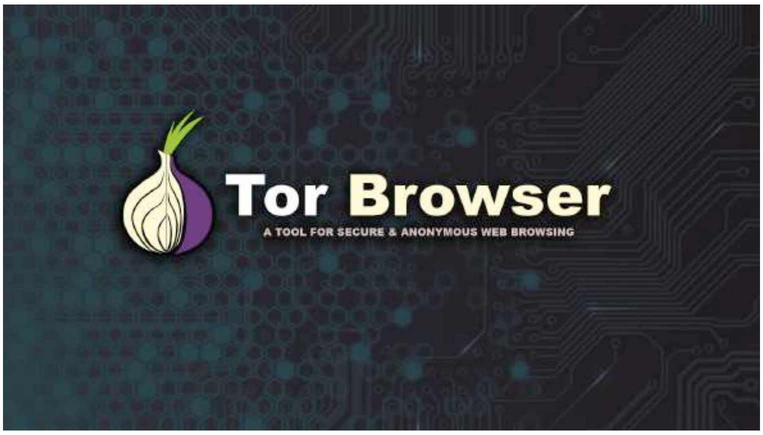
Step 4: Get well-versed in networking concepts

Knowing networking concepts and how they are created is vital for ethical hackers. Getting well-versed in various networks and protocols is beneficial in exploiting vulnerabilities. An ethical hacker with in-depth knowledge of networking tools such as Nmap, Wireshark, and others can survive the challenges in the field. Some important networking concepts are:

- TCP/IP Network
- Subnetting
- Network Masks and CIDR
- Simple Network Management Protocol
- Server Message Block
- Domain Name Service (DNS)
- Address Resolution Protocol
- Wireless Networks
- Bluetooth Networks
- SCADA Networks (Modbus)
- Automobile Networks (CAN)

Step 5: Traverse the hidden web

The part of the internet that remains hidden or is not visible to search engines is called the Dark Web. It requires special authorisation or software for access. An anonymising browser called Tor can provide access to the dark web. It is the hotbed of criminal activity, but not everything is illegal on the dark web. It also has a legitimate side, and ethical hackers must learn about the dark web and how it works.



Step 6: Add secret writing to your skill set

Cryptography or secret writing is an important asset for an ethical hacker. The art of encryption and decryption is a must in hacking. Encryption finds usage in several aspects of information security, such as authentication, data integrity, confidentiality, and more. Valuable information is always encrypted on a network, such as passwords. A hacker must learn how to identify the encryption and break it.

Step 7: Delve deeper into hacking

Once you are thorough with the topics covered so far, dive deep into hacking concepts and learn topics like SQL injections, penetration testing, vulnerability assessment, and more. Stay updated on the latest security changes in the system and the latest tools and ways for hacking and securing a system.

Step 8: Explore vulnerabilities

Vulnerabilities are weaknesses or loopholes in the system. Learn to scan systems and networks for loopholes that can lead to a security breach. Ethical hackers can also try to write their vulnerabilities and exploit the system.

Some vulnerability identification tools in the Kali Linux OS are as follows:

- **Nessus Vulnerability Scanner:** Identifies vulnerabilities on web applications and multiple systems
- **OpenVAS Vulnerability Scanner:** Identifies vulnerabilities on devices within a network
- **Nikto Vulnerability Scanner:** Acknowledges vulnerabilities on web servers
- **Nmap Vulnerability Scanner:** Identifies vulnerabilities across multiple targets
- **Wapiti Vulnerability Scanner:** Identifies web application issues like XSS and SQLi

Step 9: Experiment and practice to ace hacking

Practicing and experimenting are the keys to success in the field of hacking. Ethical hackers need to practice the learnt concepts in various environments and scenarios. Test various attacks, tools, and more.

Step 10: Attend discussions and meet expert hackers

Make a community or join forums for discussions with other hackers worldwide to exchange and share knowledge and work together. There are several communities on Discord, Facebook, Telegram, and more platforms.

How do hackers choose their victims & what they want?

Hackers choose their victims where there is a higher probability of easy financial gain. Some cyberattacks are motivated by activism and target individuals, governments, and corporations. Hackers may also be directed to attack designated targets. It's rare for cybercriminals to choose random marks.

What do cybercriminals want

Hackers are primarily out for financial gain. They aim to find the easiest targets with the most monetary return on their invested time and skill. Threat actors will typically resort to various tools to extract money from victims. Some common ways of extortion are:

- **Data ransom or exfiltration:** an attacker will lock out or encrypt a company or individual's data as a means of extortion. Examples: ransomware or selling extracted information.
- **Infrastructure theft:** an attacker will take control of information systems for use rather than destruction. Examples: crypto mining or use as a botnet.
- **Denial of service:** an attacker will prevent information systems from performing a routine operation. Example: DDoS using a botnet.

Sometimes state agencies will hire hackers to perform operations against targets deemed as enemies of the state or for intelligence gathering purposes. These attackers are generally motivated by guaranteed paydays. Government-sponsored hackers give officials plausible deniability regarding the results of attacks.

Other hackers are motivated by activism. The portmanteau, hacktivism, describes a hacker who operates to further an ideology or political agenda. They generally work as part of a collective of other engineers passionate about helping right a societal wrong.

Some hackers are purely motivated by learning the craft or for bragging rights to their attacks. The attacks themselves are the reason for the attack. The choice of their victim is only a function of exploiting a found vulnerability.

How a hacker is caught

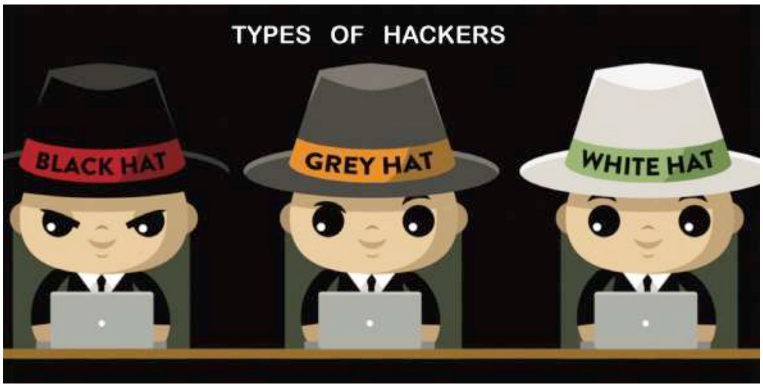
Most threat actors cover their tracks to avoid detection. These experts employ all manner of **"anti-forensic"** strategies and tactics to avoid capture. They may encrypt data before transferring it out of a system, erase or modify security logs, or run malware from RAM instead of the hard drive to avoid being caught.

Despite their best effort, here are common ways a hacker is caught:

- **Human error:** hackers are human (for now), and minor errors in execution can lead to being caught.
- **Correlation:** hackers may repeat the same successful attacks or employ strategies that reveal a pattern when reviewed over time.
- **Vanity:** hackers have or form egos during their career, which can lead to boosting their successes and being caught through this social weakness.

Only about 5% of cybercriminals are apprehended. But when a hacker is caught and arrested, there is generally, at a minimum a heavy fine. Extreme cases of cybercrime lead to years in prison, if not worse.

The luckiest of hackers may eventually reform and start using their skills to the benefit of individuals, companies, and government agencies as a White Hat. These experts become vital parts of an organisation or discover new ways to help information systems.



Dark Web hacking tools: Exploit kits for phishing, ransomware, DDoS, etc for hire

During their research, Flashpoint researchers found various types of pre-packaged exploit kits being sold on the marketplace. These automated tools allow hackers to first exploit websites and compromise visitors" browsers to carry out their attacks. Below are the kits getting a regular stream of new listings.

Ransomware exploit kit

The cheapest among the lot, the ransomware exploit kit allows hackers to exploit known vulnerabilities in applications or systems. A hacker can use them to secretly launch attacks as victims are surfing the web to inject and execute some form of ransomware. Most ransomware exploit kits rely on an array of unique code obfuscation techniques to escape detection.

Legacy ransomware

Certain dark web sellers are also offering potent forms of ransomware in a bundle deal. These bundles contain some of the most dangerous file-encrypting malware that has terrorised companies in the past, like SamSam, XiaoBa, Satan, Maniber and more. And besides ransomware, the bundles include tutorials and guides on how to conduct attacks and even exploit specific vulnerabilities.

Tailored phishing page with tutorial

The name says it all. Hackers get a tutorial for creating a custom phishing page based on their target's preferences. Victims are redirected to these pages by sending links and provoking them to click on the URLs. The hack intends to steal banking credentials, account passwords and other confidential information.

Office 365 exploit kit

This is the most expensive exploit kit on the dark web marketplace, and it's easy to understand why. Being one of Microsoft's most ubiquitous business products, Office 365 is protected by a range of advanced security technologies that are hard to exploit. As such, kits capable of crippling Office 365 defenses are classified as "premium" and often priced higher than other exploits. The kits typically work by setting up a phishing page or exploiting vulnerabilities in the Office 365 web portal.

DDoS-for-hire

The growth of DDoS-for-hire services comes at a time when Distributed-Denial-of-Service (DDoS) attacks are becoming difficult to defend against. Considering how these services are priced (typically in the range of $20-$100 per day based on duration and bandwidth requirements), many hackers can afford to invest in them to cripple the defenses of their target organisation.

The upper-tier DDoS-for-hire services include taking down larger websites via custom-crafting, which is necessary due to the widespread use of CDNs and DDoS protection improvements. In terms of popularity, DDoS-for-hire services that charge hourly rates take the top spot. Although booters remain prevalent, the need for customisation and real-time support makes subscription choices more attractive to buyers.

Buyers can also purchase advanced DDoS-for-hire services that utilise scripts to bypass private OVH and Cloudflare implementations. And a fully managed package is also available for $165.

RDP with server access

Remote Desktop Protocol (RDP) clients and server software are also in demand. Attackers can use them to execute various attacks, including payment fraud, ATOs (Account Takeover Attacks) and remain undetected while conducting their surveillance on security researchers and law enforcement agencies. Here's a list of RDP clients and server access sold on the dark web.

‣ Bank drop RDP via PayPal

Bank drops, or fraudulent bank accounts made using stolen credentials, have been used to support cash-outs and other fraud schemes in the past. Bank Drop RDP via PayPal is an exploit created using a clean RDP linked to a verified PayPal account. Hackers can use it to bypass the stringiest security measures banks have in place, with the PayPal account acting as a catalyst for account checks and other verification.

‣ Hacked RDP

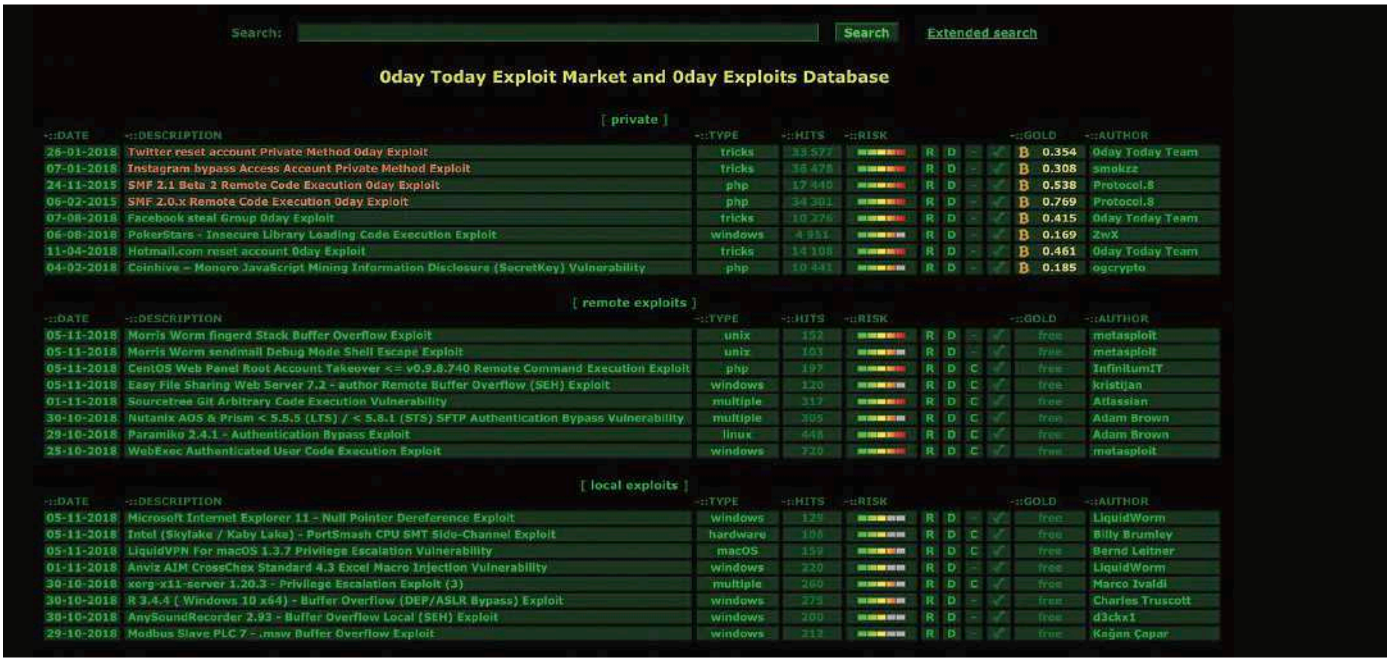
Some RDP sale items also include compromised RDP, which are predominately ports from infiltrated servers. Hackers can leverage these ports to move laterally across an organisation's network. Ports become vulnerable when they're left open due to misconfigurations or oversight. And it doesn't help that companies often leave RDP passwords as standard.

‣ Country-specific RDP

Country-specific RDP can help hackers bypass geo-blocking and carry out attacks on local organisations and governments. Flashpoint pricing analysis revealed that these RDPs go for $26 and are helpful in specific cybercrime groups.

‣ Global admin access RDP

The least expensive RDP on the list is one with global admin access. Hackers can use this to steal the sensitive data of multiple private and public organisations. As the findings from Flashpoint's research indicate, data like bank logs, payment card information and digital copies of government-issued IDs carry a decent price tag. Hackers can list the spoofed credentials on the dark web or even hold them and demand ransom from victim organisations. ■



Oday Today Exploit Market and Oday Exploits Database

[private]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
26-01-2018	Twitter reset account Private Method Oday Exploit	tricks	33 577		R	D	-	✓	₿ 0.354	Oday Today Team
07-01-2018	Instagram bypass Access Account Private Method Exploit	tricks	36 478		R	D	-	✓	₿ 0.308	smokzz
24-11-2015	SMF 2.1 Beta 2 Remote Code Execution Oday Exploit	php	17 440		R	D	-	✓	₿ 0.538	Protocol.8
06-02-2015	SMF 2.0.x Remote Code Execution Oday Exploit	php	34 301		R	D	-	✓	₿ 0.769	Protocol.8
07-08-2018	Facebook steal Group Oday Exploit	tricks	10 276		R	D	-	✓	₿ 0.415	Oday Today Team
06-08-2018	PokerStars - Insecure Library Loading Code Execution Exploit	windows	4 951		R	D	-	✓	₿ 0.169	ZwX
11-04-2018	Hotmail.com reset account Oday Exploit	tricks	14 108		R	D	-	✓	₿ 0.461	Oday Today Team
04-02-2018	Coinhive – Monoro JavaScript Mining Information Disclosure (SecretKey) Vulnerability	php	10 441		R	D	-	✓	₿ 0.185	ogcrypto

[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
05-11-2018	Morris Worm fingerd Stack Buffer Overflow Exploit	unix	152		R	D	-	✓	free	metasploit
05-11-2018	Morris Worm sendmail Debug Mode Shell Escape Exploit	unix	103		R	D	-	✓	free	metasploit
05-11-2018	CentOS Web Panel Root Account Takeover <= v0.9.8.740 Remote Command Execution Exploit	php	197		R	D	C	✓	free	InfinitumIT
05-11-2018	Easy File Sharing Web Server 7.2 - author Remote Buffer Overflow (SEH) Exploit	windows	120		R	D	C	✓	free	kristijan
01-11-2018	Sourcetree Git Arbitrary Code Execution Vulnerability	multiple	317		R	D	C	✓	free	Atlassian
30-10-2018	Nutanix AOS & Prism < 5.5.5 (LTS) / < 5.8.1 (STS) SFTP Authentication Bypass Vulnerability	multiple	305		R	D	C	✓	free	Adam Brown
29-10-2018	Paramiko 2.4.1 - Authentication Bypass Exploit	linux	448		R	D	C	✓	free	Adam Brown
25-10-2018	WebExec Authenticated User Code Execution Exploit	windows	720		R	D	C	✓	free	metasploit

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
05-11-2018	Microsoft Internet Explorer 11 - Null Pointer Dereference Exploit	windows	129		R	D	-	✓	free	LiquidWorm
05-11-2018	Intel (Skylake / Kaby Lake) - PortSmash CPU SMT Side-Channel Exploit	hardware	108		R	D	C	✓	free	Billy Brumley
05-11-2018	LiquidVPN For macOS 1.3.7 Privilege Escalation Vulnerability	macOS	159		R	D	C	✓	free	Bernd Leitner
01-11-2018	Anviz AIM CrossChex Standard 4.3 Excel Macro Injection Vulnerability	windows	220		R	D	-	✓	free	LiquidWorm
30-10-2018	xorg-x11-server 1.20.3 - Privilege Escalation Exploit (3)	multiple	260		R	D	C	✓	free	Marco Ivaldi
30-10-2018	R 3.4.4 (Windows 10 x64) - Buffer Overflow (DEP/ASLR Bypass) Exploit	windows	275		R	D	-	✓	free	Charles Truscott
30-10-2018	AnySoundRecorder 2.93 - Buffer Overflow Local (SEH) Exploit	windows	200		R	D	-	✓	free	d3ckx1
29-10-2018	Modbus Slave PLC 7 - .msw Buffer Overflow Exploit	windows	212		R	D	-	✓	free	Kağan Çapar

A Hackers World: How they think and behave

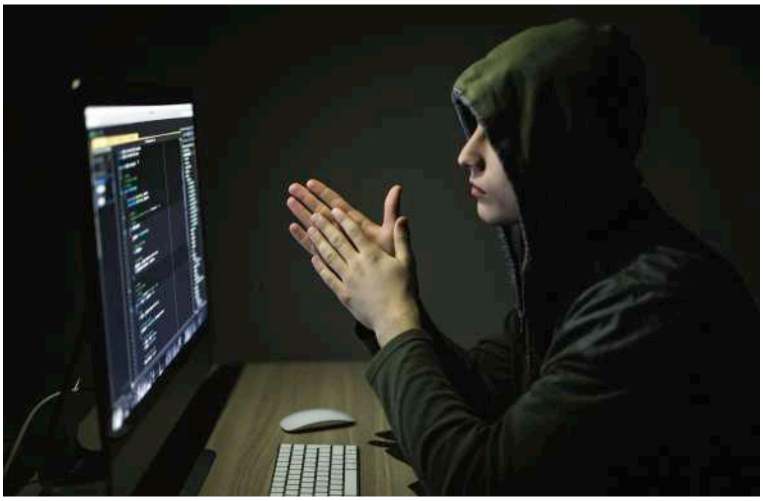
An easy life for a hacker – if you know where to look.

Author: Raj Meghani

The word "Hacker" sends chills down anyone's back and even moreso when you have been subjected to any one of the thousands of cyber-attacks that we are seeing almost on a daily basis now globally.

The scary thing is nowadays, it's becoming a word that fits into the norm. Every day we hear about some organisation being compromised by hackers and whilst the press does their fair share in amplifying these attacks, the word "Hacker" has almost become as ordinary as the word "Victim".

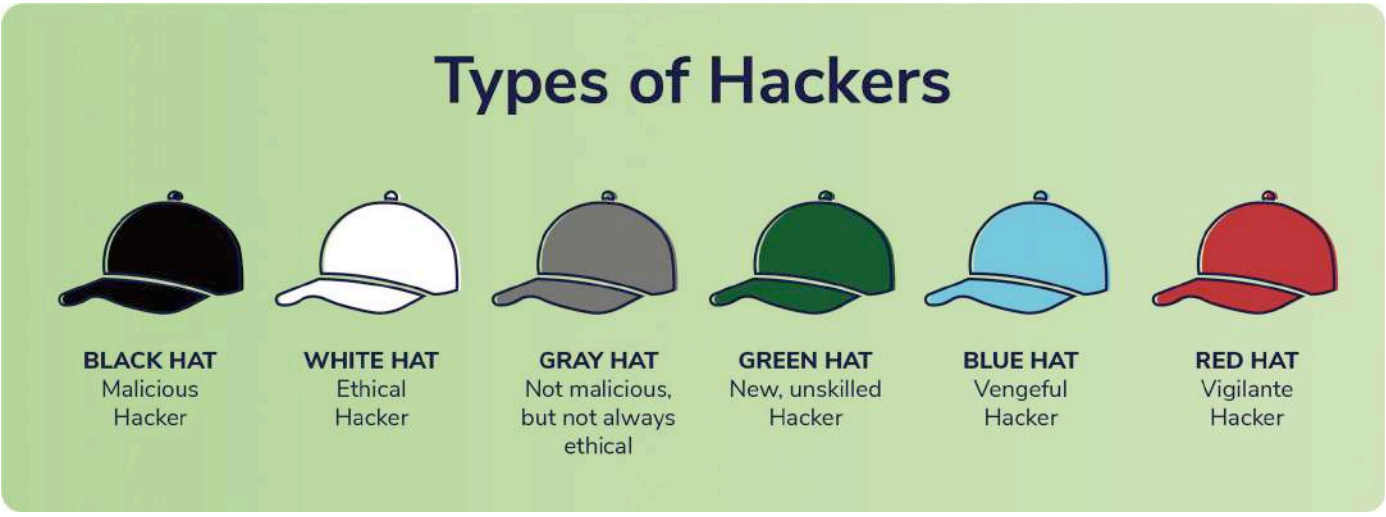
But the Hacker comes in all shapes and forms – let's quickly recap before I delve into the darker side of how easy it is for a hacker nowadays to cause widespread disruption.



1. The Malicious Hacker – Black Hat

This is the dangerous criminal to watch out for. This hacker's sole motive is to disrupt operations, destroy and create panic whilst looking to gain anonymous notoriety and a financial gain.

Blackmail features high on this list whether it's Ransomware or Insider Threat. Stealing data is at the heart of most attacks – violating privacy of this data, bringing widespread chaos to disable communication systems, like we saw recently in my LinkedIn posts with NHS, Uber and Philippine Airlines.



2. The Wannabe Hacker - Green Hat

The Green Hat hacker is on the ladder to becoming a full-blown malicious hacker. They are avid listeners and inquisitive in nature with the intent to create damage. Think of these as being on the waiting list of the Black Hat – they are watching, learning and honing their skills until they make the grade…

3. The Angry Hacker – Blue Hat

These hackers are beginning their journey on a dangerous, slippery slope but they don't care. They are not interested in learning about the latest sophisticated way to hack an organisation or cause disruption to critical infrastructures. That's too laborious and hard work. They are like 'Script Kiddies' who copy codes and use them to inundate websites with DDoS attacks. They are angry and want revenge for whatever reason – with minimal effort.

4. The Undecided Hacker – Grey Hat

Things can be black and white. And then somewhere in between is the grey area.

These are the undecided – not necessarily hacking for malicious intent for their own personal gain but then not strictly authorised to compromise an organisation's systems. Sits on the fence…. until personal gain wins and the hacker moves to the dark side.

5. The Nation State Hacker

Nation sponsored or state hackers are politically motivated. Think Russia with the ongoing Ukraine war. They are often appointed by States who want to get access to sensitive, classified government intelligence on other countries which can give them a competitive edge – politically, economically, financially, and socially.

This is different to a "Hactivist" who will target a government's network and communication systems to further their own political or social agenda.

6. The Ethical Hacker – White Hat

These are the good people with a pure agenda. These white hat hackers are serious cybersecurity know-it-alls who are subject matter experts in identifying vulnerabilities and loopholes for organisations and institutions. They are widely sought after and are our protectors and a Black Hat's nightmare.

7. The Relentless Hacker – Red Hat

These are the Black Hat's worst nightmare as they are ruthless and relentless in trying to figure out how the malicious hacker has compromised an organisation. That's how they differ from the White Hat hackers mentioned above. It's their mantra and modus operandi to get the malicious hacker to crumble and/or make their life difficult so they are having to constantly change their strategy and tactics.

So there we have it – the good and bad hackers (although I suspect there are others out there not mentioned here and more worryingly the new style hackers of tomorrow we have still yet to discover….)

I am fascinated yet disturbed by the mind of the malicious hacker. Whilst I can take an educated guess on the motives, etc, it never fails to astound me how much is out there for sale on the dark web and hacktivist forums making any hackers job easy.

BIO

Raj Meghani is Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. Raj is Editor for Cybersecurity Trends UK which has a global presence and is active in thought leadership and knowledge transfer of cybersecurity and business risk management.

LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

Tools and cyber-attack kits used for ***phishing, ransomware, DDoS, and others*** are increasingly being sold on the dark web with low barrier to entry prices – scarily starting from as little as $5 (Atlas VPN research). These are targeted to the unprofessional hackers who want the easy way out without doing heavy lifting on ramping up their technical skills. Social Engineering, Ransomware-as-a-service (RaaS) are fast track preferences today for those hackers wanting to do maximum damage in minimal time. All at a cost which quite frankly starts at less than the cost of a couple of coffees.

10
Malware Attack
1
Denial-of-Service
9
Birthday Attack
2
Man-in-the-Middle (MitM) Attack
8
Eavesdropping Attack
3
Phishing Attack
7
SQL Injection Attack
4
Drive-by Attack
6
Cross-Site Scripting Attack
5
Password Attack

The Dark Web is called that for a reason. It's crossing from our everyday browser we use to the Dark Web which is one of the Go-To marketplaces hackers, terrorists, human traffickers, etc look to network, buy, source, extort anything which is effectively illegal – at a price. Of course, there are others who may have a legitimate reason and want anonymity but my focus here is on the cyber criminals.

HP Wolf Security and Forensic Pathways' research report found that 76% of advertisements for malware and 91% for exploits are listed on the Dark Web for under $10. Furthermore, the average cost of compromised Remote Desktop Protocol stolen credentials is just $5.

Malware like Ransomware-as-a-Service (RaaS) kits have made it so easy for hackers to venture into this area – almost 44% of them purchased on the Dark Web are effectively launched to their unsuspecting victims for extortion of money. Shameful today and unfortunately, an increasing trend as we've seen with recent targeted ransomware attacks.

Even known vulnerabilities or loopholes in current operating systems, software, web-based applications, etc are for sale giving the hackers a wider surface attack area. What's worse is that where these vulnerabilities have not yet been uncovered in the main, there is a ready hacker open to paying 5 figure sums upwards to manipulate and exploit targeted high/ultrahigh net worth/high profile victims and organisations.

I read a very interesting articles by TechRepublic and Privacy Affairs which had some unbelievable stats on the Dark Web – check them out:

- Credit card data with an account balance of up to $5,000 = $120, 1 UK credit card with CVV = $20.
- 1 x PayPal stolen account with $1,000 - $3,000 balance = $45
- 1 x hacked Twitter account = $25; 1 x hacked Facebook account = $45; 1 x hacked Gmail account = $65
- 1 x EU passport = $3,800
- Fake cryptocurrency blockchain account (using fake IDs) = $90; Binance verified account = $260
- Corporate entities network access = $2,000 - $4,000
- 10million US email addresses = $120
- DDoS attacks:
  - Unprotected target website can be hit at 10,000 to 50,000 requests **per second for an hour** for as low as $10 or $850 per month
  - Protected websites can be hit with 20,000 to 50,000 requests **per second, using multiple elite proxies** for $200 per day.
- A Remote Access Trojan (RAT) which allows full access and control to another device = $5 - $45
- Ransomware base kit = $15 - $76
- Whaling phishing kit = $7
- Password cracking pack = $10

The list goes on and is not exhaustive by any stretch of the imagination.

I send a clear message to the victims and to those who will be attacked in some shape or form in the future – take extra care in protecting your sensitive information & credentials.

Once stolen, the cost of buying them on the Dark Web, as we can see from the above stats, is negligible. The cost of recovering from being a victim could have profound and much larger ramifications. ■

Game on: Why iGaming is a hot target for hackers and how to protect your business.

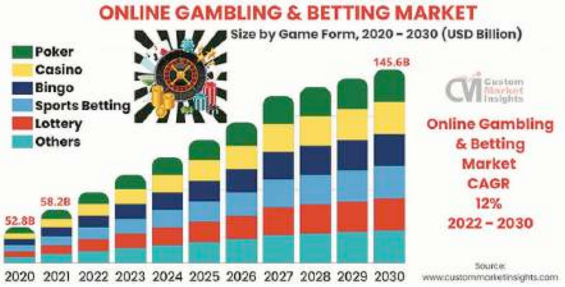
Author: Christene Best

The iGaming industry has always been attractive for hackers: it doesn't take a lot of resources to plan an online casino heist in the digital space and at the same time cybercriminals can reap big payoffs with just a few tools or tricks.

During COVID-19 lockdowns, when casinos closed, gamblers turned to online gaming sites. According to UK research (1), regular gamblers were six times more likely to gamble online compared to before the pandemic. In the US, the online gambling and betting market was worth around $61.5 billion USD in 2021 and is estimated to grow to $114.4 billion by 2028 (2).

BIO

Chris is Vice President of Marketing & Channel Development for INETCO Systems Ltd. INETCO provides real-time transaction monitoring, cybersecurity protection and payment fraud protection for payment networks, card issuers & acquirers and merchants. Chris has led marketing, sales, customer success and tech support teams for companies ranging in size from startup to Fortune 500. She has worked for companies including Xerox Canada, Fincentric Corporation, Klein Systems Group, Beanworks and AMPD Technologies. Chris has been a volunteer mentor for tech startups through New Ventures BC since 2010. She earned a B.A. (Hons) in Political Studies, and an MBA from Queen's University in Kingston, Ontario.



This market growth has attracted the attention of hackers who see both lucrative opportunities and vulnerabilities in the digital environment. Instead of fake chips, counterfeit bills, and slot cheats of the real-life casinos, today's cybercriminals use Dedicated Denial of Service (DDoS) attacks and user account fraud to attack online gaming sites (3).

While real-world gambling houses need strong physical security and surveillance, for online sites their resilience to crime now depends upon strategies and measures designed by their cybersecurity experts.

New challenges and new tools in fighting cybercrime

According to research (4), more than 76 percent of Q3 2020 cyber attacks targeted online gaming and gambling. In 2020, SBTech's platform was taken down in a ransomware attack. The shut down affected hundreds of third-party websites that utilised SBTech's platform to run their sports betting and online casino services. In the same year, popular gambling app Clubillion became a victim of hackers (5) who exposed 200 million records of customer information per day and made the app's users vulnerable to banking frauds and other possible cyber attacks.

While many iGaming companies might have invested in cybersecurity tools in the past, 2022 brought in new challenges that spurred businesses to overhaul their cybersecurity strategies.

Intelligent bots powered by AI have become good at mimicking human behaviour and are three times harder to detect. The Russian invasion of Ukraine brought in an increase in the number of state-sponsored actors targeting critical infrastructure with DDoS attacks. At the same time, businesses face a completely new pool of pandemic-generated citizen fraudsters and cybercriminals.

How can iGaming companies stay resilient to hacking? Here are a few strategies that will help businesses protect their online presence and revenue.

1. Ensure multi-layered cybersecurity to prevent interruptions from DDoS and bot attacks

Online gambling and sports betting site operators face pressure to have their sites always available. On betting sites, transactions are made in real-time, so even a small slowdown can result in visitors leaving for a competitor's site. DDoS attacks can disrupt a site's availability for hours or days and cost businesses up to $40,000 per hour.

Hackers can initiate DDoS attacks on multiple layers, making it hard to detect and block them. In an application layer attack, application services or databases get overloaded with a high volume of application calls. Attacks targeting network layer or transport layer protocols overwhelm target resources.

Application layer DDoS attacks are some of the most difficult attacks to mitigate because they **mimic normal user behaviour** and are harder to identify. They can bypass even industry-leading firewalls and biometric protections.

To stay resilient to these types of threats, iGaming businesses can use real-time payment monitoring tools with behavioral analytics that leverage data not only from the network and applications but also from the application payload.

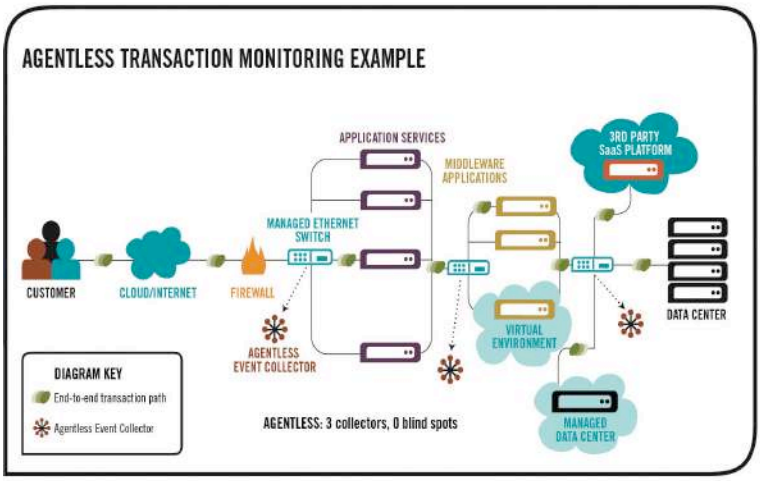
2. Block cybercriminals, not revenue

Traditional cybersecurity solutions can be slow in detecting new and emerging cyberattacks and they experience an even bigger challenge in blocking the crime. Traditional firewalls can only block traffic at the IP address and port level of the network. That means that in case of a DDoS attack or other high-velocity attacks, the firewall will block legitimate customers coming from the same IP address or port. This results in high amounts of false positives, angry customers, and lost revenue.

Newer cybersecurity solutions leverage both unsupervised and supervised machine learning to identify emerging threats and build individual customer profiles on the fly. Through self-learning, machine learning models are updated automatically and they can assign a risk score for a transaction in milliseconds and block only the criminal activity, keeping legitimate transactions unaffected.

3. Protect gamer's accounts

Revenue isn't the only thing that can be lost due to cyber attacks. The gambling and betting businesses also store their players' personal and payment data which may also be targeted by criminals. Bad actors can takeover user accounts or commit other identity-based attacks. It's the responsibility of a business to ensure the security of its players' accounts and any mistake can cause serious reputational damage.



Continuous real-time screening and transaction monitoring with automatic risk-scoring can help iGaming companies identify suspicious behavioural patterns and anomalies and automatically block them before they damage the brand.

4. Stay on top of your weak links in the system

While investing in cybersecurity tools and building the right team are essential, it's still important to regularly analyse vulnerabilities or weak links in the system. An online gambling company might have great player authentication solutions, but miss some other important pieces of the security puzzle.

Does your business have all the right data, when you need it? Is it available instantly? Do you have protection on multiple layers, including your network and applications? Are you monitoring for the correct types of threats? If these questions are included in a regular review with your team, you can stay vigilant against emerging threats.

5. Secure cryptocurrency and digital payments

As more and more companies accept cryptocurrencies for sports bets and online gambling, keeping digital currency protected should be included in the cybersecurity strategy. If you can use the same tools for fraud detection and monitoring digital transactions from one platform that provides your team with access to real-time data, you can stay ahead of bad actors and keep their hands out of your business' pockets.

6. Stay compliant

The gambling industry is highly regulated. Businesses are required to ensure compliance with Know Your Customer (KYC) and Know Your Supplier (KYS) regulations. Online gambling operators also must implement strong anti-money laundering (AML) procedures to avoid penalties and in some countries, report incidents of cyberattacks.

Real-time transaction monitoring with machine learning and behavioural analytics will enhance the protection of the iGaming business, automatically separating bad actors and suspicious activity from legitimate players and visitors. As many digital transactions are instant and irrevocable, your cybersecurity tools should be able to keep up the pace and help minimise business risks. ■

Have specific questions about the cybersecurity of your payments and iGaming business? To find out more, you can contact Chris at https://www.linkedin.com/in/christene-best/

(1) Alan Emond, Agnes Nairn, Sharon Collard, Linda Hollén. Gambling by Young Adults in the UK During COVID-19 Lockdown. Journal of Gambling Studies, 2021; DOI: 10.1007/s10899-021-10029-y

(2) Recent Trends in Global Online Gambling & Betting Market Size & Share to Exceed US$ 114.4 Bilion, at 10.9% CAGR Rise by 2028 - Industry Analysis, Trends, Forecast Report by ZMR; available at: https://www.prnewswire.com/news-releases/recent-trends-in-global-online-gambling--betting-market-size--share-to-exceed-us-114-4-bilion-at-10-9-cagr-rise-by-2028---industry-analysis-trends-forecast-report-by-zmr-301542610.html

(3) Online Gaming is a Hotbed for DDoS Attacks, According to Nexusguard Research; https://www.businesswire.com/news/home/20201215005432/en/Online-Gaming-is-a-Hotbed-for-DDoS-Attacks-According-to-Nexusguard-Research

(4) C. Cimpanu, Gambling company to set aside $30 million to deal with cyber-attack fallout; https://www.zdnet.com/article/gambling-company-to-set-aside-30-million-to-deal-with-cyber-attack-fallout/

(5) Cyber Threats of Online Gambling | Five Online Gambling Platform Breaches to Learn From; https://eclypses.com/news/cyber-threats-of-online-gambling/

A hackers world - Killing the Zombie dead.

Author: Marco Essomba

I was called by a client to investigate a strange behaviour in their network infrastructure. It turned out to be a major cybersecurity breach. Of course, I cannot disclose the full details of the incident as Non-Disclosure Agreement rules apply. But I wanted to share some lessons an d tips learned from that incident to help network and security administrators.

BIO

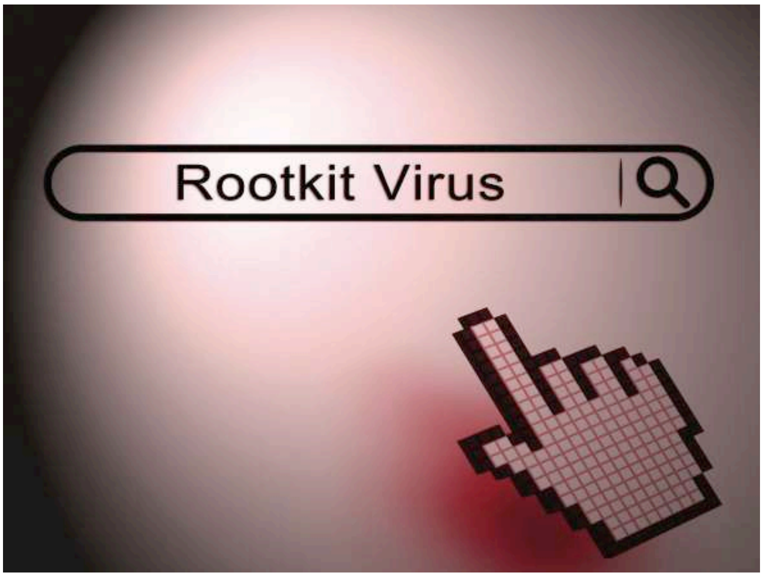
Marco Essomba is the Founder & CTO of BlockAPT – a UK based innovative cybersecurity company.
An influential thought leader in cybersecurity with almost 2 decades of working with some of the largest and well known institutions. Marco's passion, expertise and knowledge has culminated in the design of the unique central management, command and control BlockAPT platform which allows businesses to stay ahead of cyber threats 24/7.
Marco is often called upon as a panellist at cybersecurity conferences and has been a host ambassador at CyberTalks, one of London's largest cybersecurity events. With 16,000+ followers on LinkedIn and 35,000+ on Twitter, he is sought after for his quick problem-solving approach and helping businesses futureproof their security infrastructure.

To find out more about BlockAPT, please visit https://www.blockapt.com
To find out more about Marco Essomba, please visit https://www.linkedin.com/in/marcoessomba/ or https://twitter.com/marcoessomba

How strange is weird?

It all started with a strange behaviour on the core network infrastructure. Why should a routing device at the core of the network attempt to make regular outbound DNS requests to IP addresses that appear to be random home computers in Asia?

Moreover, it is not usual to have core routers attempt to make constant HTTP requests to unknown home computers in Eastern Europe and then flood their own local network with DDoS attacks to bring down critical network services. These are some of the strange symptoms that caught my attention.



Paranoid Rootkit

Further investigation using sys-admin and network tracing tools revealed that some of the core network devices had been compromised.

The attacker installed a kernel rootkit that took over the network stack of those devices allowing full control of those devices. Compromised devices were allowed to join a global botnet that was using several command and control centres spread around the globe. Further 'Cyber Crime Scene Investigation' (CCSI) was required to get to the bottom of what this rootkit was up to.

CCSI Miami

Having established the root cause of the strange network behaviour, the challenge was now to gather and analyse all the information to better understand what else could have been infected in the core network. The rootkit malware seemed to have some sort of awareness about its local network surroundings.

With full control of the infected device network stack, the malware was able to monitor local activities and decide when, how, and what to connect to in order to obtain further commands under certain conditions.

By simulating the right conditions, the malware was able to trigger and replicate several of its assaults on the local network. This allowed the collection of useful information for analysis, including traffic patterns, botnet architecture, and trigger conditions that provided a definitive answer of the inner workings of the malware rootkit.

Killing the zombie device dead

Following a detailed analysis of network traces and system processes behaviour on the compromised device, it was clear that this device was now a fully grown 'zombie' and had to be given a new life. Having collected all the evidence, a fresh and clean install was required to ensure no traces remained from the earlier breach. Cleaning up the offending device was just the start. Ensuring that the rootkit had not infected any other network components was crucial.

A thorough analysis and monitoring of the whole network infrastructure and lock down was required to ensure that the malware was completely removed and cleanse. Of course, the lessons learned highlighted below, had to be applied in order to strengthen the security of the overall infrastructure and reduce the likelihood of such a breach occurring again in the future.

Lessons learned

From this incident, I have drawn 7 lessons. Most of which are common sense guidelines to cybersecurity defence-in-depth strategies. Cybersecurity is an on-going battle between technology, people, and processes. The three must work together to ensure that network infrastructures and applications remain secure and always available. Here are some guidelines that network & security administrators can apply to strengthen their networks:

1. Tightly control remote access: Never allow access to a network device from the Internet without strong authentication. Always use 2-factor authentication with a strict Access Control List (ACL) to restrict what, where, when, and who can manage critical network devices.

2. Defend in many layers: A defence-in-depth architecture should be followed to strengthen the security of the overall network infrastructure. By doing so, this will greatly reduce the risk of a single component infecting the entire network infrastructure. For example, at the technology layer, a combination of next generation firewalls at the edge of the network, intrusion detection systems, and advanced endpoint detection and response is a minimum requirement.

3. Monitor, detect, and remediate: A robust monitoring, detection, remediation system and processes should be in place to establish a baseline of normal network traffic behaviour. From that baseline, anomalies can be detected quickly, and remediation applied promptly. Security analytics must play a key role here.

4. Plan and prepare for remediation: The question is not if a network will be hacked but when. Given enough time, any network can be hacked, therefore it is necessary to have regular drills and a clear response plan to prepare for a major breach.

5. The cyber battle never stops: Cybersecurity is an on-going battle between people, processes, and technology. Technology alone cannot guarantee cybersecurity but a mix of the three will provide the strongest cyber defence.

6. Tightly control all inbound and outbound flows: Most companies strongly control inbound access to their network infrastructure and services, but often, outbound access to is left unchecked. By putting in place strict rules for outbound connectivity a single device breach will remain isolated and reduce the chance of a malware infection spreading throughout the network. For a malware rootkit, this means starving it from connecting to its control and command centres and stopping it from downloading further commands as a stepping-stone to amplify its attacks.

7. Establish a secure baseline of device build: All network devices should be hardened and added to the network with a secure baseline to ensure consistency and to avoid basic mistakes. This procedure should be much stricter for all Internet facing devices.

Conclusion

This quote from Robert Mueller illustrates the challenge that network & security administrators face to protect their digital assets.

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." ~

Robert S. Mueller, III Director Federal Bureau of Investigation

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

The question of a cyber breach for any network infrastructure connected to the internet is not if but when. Therefore, by putting in place the right controls from a technology point of view, cyber-attacks can be detected swiftly and stopped before damage is done. Moreover, people and processes play a key role in strengthening the security posture of an organisation, therefore, continuous training and process tuning to adapt to the constantly changing cyber threats is key. ■

BLOCKAPT™

MicroToken Exchange (MTE®) Technology

The next level quantum-safe or quantum-resistant data protection and secure communication capabilities.

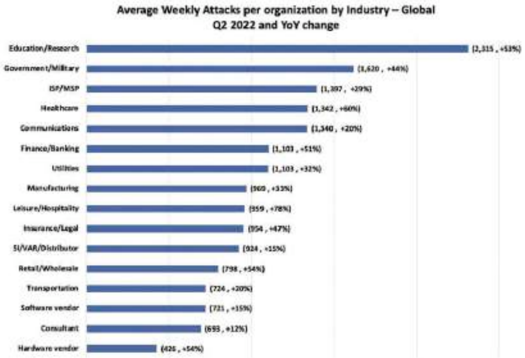
- **FIPS 140-3** validated standard technology
- Requires no changes to **user experience**
- A **real-time** command & control panel
- Satisfy **data protection compliance** standards
- **Secures** data inside the platform with a layered defence
- Fully secured **2-way channel** for communications

blockapt.com

Victims of cyber-attacks: The destruction cyber-attacks leave and the pressures victims face.

Author: Joe Jeanjaquet, Senior Director of Applied Technology at Eclypses

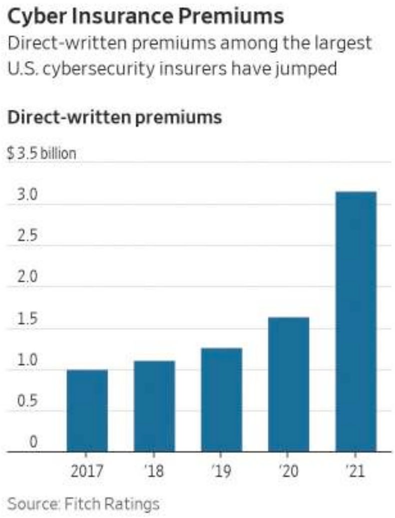
It is a strong possibility that another cyber-attack happened today. As of October 1st, 2022, the Center for Strategic & International Studies has documented 96 significant cyber incidents on Government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars during 2022. Yet, while the instances of cybercrime is up 600% since the beginning of the pandemic, there is still much we can do to reverse that trend line. It can seem insurmountable. It can seem inevitable.



The victims are not nameless, faceless organisations but ordinary citizens like you and me holding the bill.

How do cyber-attacks disrupt people’s lives?

At the risk of generalisation, cybercrime is never victimless. It is common to justify actions of perceived justice or without monetary gain as harmless or even just. The reality is when companies are attacked, cyber insurance for others increase.



When nations are attacked, budgets are reallocated, and other services suffer. When personal data is taken, reputation is irreparably broken, and the cost of customer retention and net-new users swells.

Whether cybercriminals realise the cost, or outright do not care, the scale of victimhood has changed. In 2022, we saw the infamous Conti Ransomware attack on the Costa Rican Government. We know that the Costa Rican Ministry of Science, Technology and Telecommunications of Costa Rica (MICITT) is currently dealing with the fallout of a cyber-attack on their essential government services on April 15, 2022. The fine people of that country were left with no recourse when the

Costa Rica declara el estado de emergencia por el ciberataque de Conti ministry was forced to shut down the entire network to stop the bleeding, leaving the entire population without access to health, education, and monetary services for weeks. We can only hope that their refusal to pay the ransom will be a positive step in dissuading future attempts against other nations.

In the end, some victims are victimised over and over as a result. Credential stuffing is a remarkably simple form of brute force cyber-attacks in which criminals use stolen usernames and passwords to access user accounts in other systems. It is one of the most common causes of data breaches for a simple reason: stolen usernames and passwords are cheap, accessible, and they work. As more credentials are exposed through breaches, credential stuffing attacks are increasing.

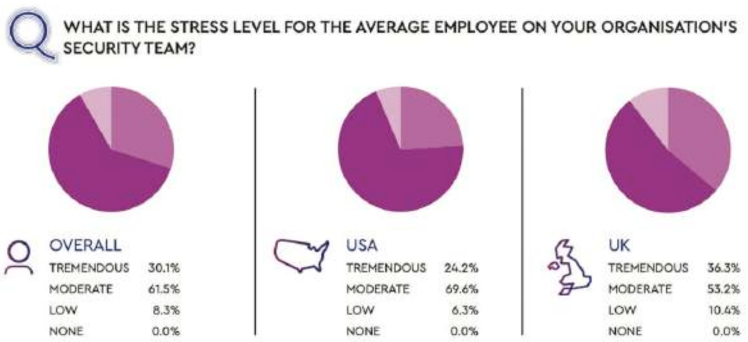
What kinds of pressures do CISOs carry these days?

With these attacks becoming commonplace, a growing, albeit lesser, consequence is the personal and professional stress induced by the uncertainty.

When asked which technical facet of the job drives the most stress, CISOs pointed the finger at "staying ahead of threats" (33%), securing the network (28%), and securing endpoints (26%). (Balbix)

Twenty-five percent (25%) think the job has had an impact on their mental or physical health (or both), as well as their personal and family relationships. (Balbix)

100% of CISOs surveyed find their role stressful, with 91% saying they suffer moderate or high stress. (Balbix)



Eighty-eight percent (88%) of CISOs are doing more than the average 40-hour work week, with 60% saying they rarely disconnect. (Balbix)

As a result, companies and other organisations sacrifice efficiency for the necessary, potentially restrictive additions to core architecture. Cybercrime is a reality of life, but it wastes so many cycles that could be spent on productivity. In a way, the biggest victim of cyber-attacks is our future.

How should victims secure their systems without relying on new tech?

Since a magic, 'fix-all-security-issues' security tool is unlikely to exist, the battle is never-ending. The good news is that by changing the way we think, our philosophies are maturing and are making a significant difference.

- **Education:**

Unfortunately, relying on users to make good decisions is never a good bet. On the other hand, a single training session might save millions overall.

BIO

With over a decade of technical and leadership experience, Joe Jeanjaquet is Eclypses' Senior Director of Applied Technologies. Across his career, Joe has worked as a developer, creating web applications and managing databases and reports for a wide variety of clients. At Eclypses, Joe leads the Applied Technologies team, overseeing implementation and application of Eclypses' MTE technology in client and partner applications. Joe works directly with the Executive Team to develop the technical requirements for innovation and execution in the mobile data security market.

Implement password managers and good practices. Teach people to inspect links and to verify requests for information. Instruct people not to trust implicitly.

- **Zero Trust security policies:**

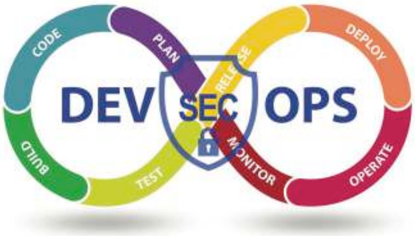
An architecture based on the philosophy that nothing - no device, user, or application attempting to access our architecture - will ever be considered secure. On average, zero trust security policies saved $1.76 million per breach (PurpleSec).

Expanding on this a little bit, the idea that you should never trust anything you do not control can also be a valuable strategy and contrasts with recent trends regarding multi-packet, open-source dependencies and 'bolt-on' security. In some cases, this might mean that we should not trust our operating systems or our expensive security tools.

- **DevSecOps:**

DevSecOps stands for development, security, and operations. It blends process, culture, and tooling to integrate security as the responsibility of all members in the IT (Information Technology) lifecycle. To narrow it down to the biggest differences:

It puts security first by introducing it immediately in the Software Development Lifecycle (SDLC) by the **developers**.



- DevSecOps is about **built-in security,** not "bolt-on security" that functions as a perimeter around apps and data.
- Everyone involved has an obligation to security in the DevOps continuous integration and continuous delivery (CI/CD) workflow.

DevSecOps attempts to deliver secure applications as quickly as possible.

- **Application-level security:**

If it makes sense to slide the responsibility for security from the IT team to the Application Developer, then it also makes sense to slide the responsibility of data security from the transport layer to the application. Truly, if the data is the most valuable part of the application, then it should be our desire to protect it as soon as possible, in the application, and secure it until it is consumed or stored.

By combining the philosophy of zero trust with application toolsets that are validated, quantum resistant and able to provide consistent security for all applications and appliances throughout your entire network, it is possible to remove trust in the things we do not control, build the security in from the beginning, and protect our applications against future threats.

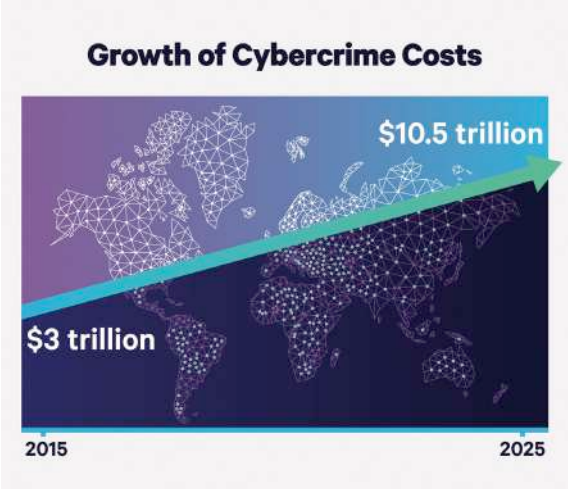
Conclusion

The future will be better because of the changes we are making right now. It is unlikely that cybercrime can be prevented but we can change the way we think. We should find inspiration in the victims of cybercrime because it is to them, we owe our effort. If we cannot be perfect, we can at least be a little bit better. If our efforts today seem futile, we could be saving ourselves time and effort tomorrow. And somewhere down the road, a policy with your name on it might have saved someone from being a victim. ■

Ten steps to reduce cyber criminals' ROI.

Author: Erik Alfonso Nilsen

Cybercrime is on the rise, data breaches are increasingly common, and cyber criminals are becoming more brazen and sophisticated in their attacks.



However, there are simple steps that you, including novices to experts can take to reduce the risk of becoming a cybercrime victim by making it much harder for criminals to target and exploit your property.

1. Be aware of the risks.

The first step to protecting yourself from cybercrime is to be aware of the risks. Keep up to date with the latest news on data breaches and cyberattacks and learn about the different types of cybercrime. Spending just an hour per week reading reputable articles online can work wonders, and, even after a few weeks, you will better understand the threat landscape and your vulnerabilities.

2. Use strong passwords & opt into 2FA.

One of the most effective ways to protect your online accounts is to use strong passwords and opt-in to two-factor authentication (2FA). A strong password should be at least 8 characters long and should include a mix of upper and lower case letters, numbers, and special characters. Avoid using easily guessed words like a name or date of birth for you, your significant other, or any children. When 2FA is enabled, you are required to provide two forms of authentication – usually a password and a code that is sent to a mobile device – before you can access an online account; 2FA can frustrate sophisticated hackers enough such that they move from you to someone who has not opted in.

3. Keep your software up to date.

Another important security measure is to keep your software up to date. This includes your operating system, web browser, plugins, and any applications you have installed on any computer or device that connects to a network, ranging from an isolated local network to one linked to the

World Wide Web. Outdated software often contains security vulnerabilities that bad actors exploit to gain access to your network-connected property including the information residing within it.

4. Use a secure connection.

Whenever possible, utilise a secure connection when accessing websites or other information online. This means a VPN or only connecting to secure websites using HTTPS; if you connect to a website without a VPN and do not see a padlock symbol on the left side of the URL address bar, it is best to, as quickly as possible, close the browser or navigate to a secure website. This will help to protect your system from a hostile takeover and prevent private data from being accessed, stolen, or corrupted by unauthorised third parties.

5. Be cautious with email attachments.

Email attachments are a common way for cyber criminals to spread malware. Be cautious when opening email attachments, even if they appear to come from a trusted sender. If you're not expecting an attachment, or if the email looks suspicious in any way, it's best to delete it prior to opening.

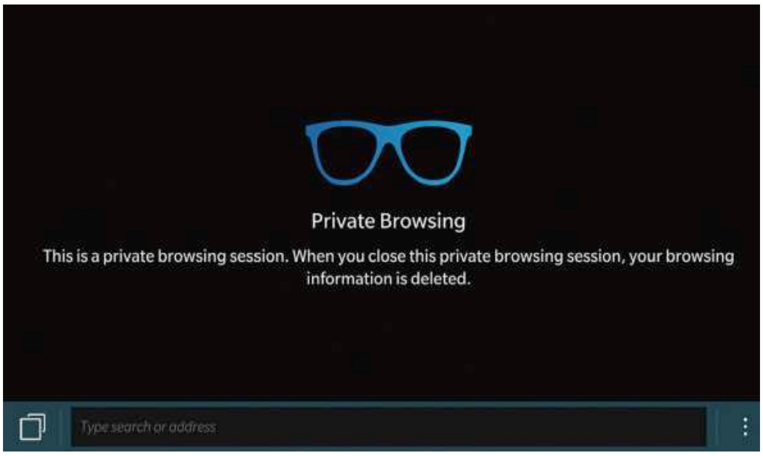
6. Keep personal information private.

Be careful about the personal information you share online and at least password protect confidential data, so it isn't low hanging fruit for invaders. Think twice before posting anything that could potentially identify you, such as your full name, date of birth or home address. Cyber criminals can use this, and sometimes considerably less, information to steal your identity and target you directly for fraud and other nefarious purposes.

7. Monitor your financial activity.

Regularly check your bank/credit card statements and credit report for any suspicious activity. This could be a sign that your personal information

has been compromised. If you spot anything out of the ordinary, report it to your bank or the relevant authorities immediately.


Private Browsing

This is a private browsing session. When you close this private browsing session, your browsing information is deleted.

8. Use security features.

Most devices and applications come with built-in security features that can help protect you against cybercrime. For example, many browsers now have a "Private Browsing" mode that stops your browsing history from being saved. Make sure you take advantage of these and other such features when available.

9. Be careful what you click on.

Links in email messages, social media posts, and online ads can often be malicious. If you click on a link that leads to a malware-infected website, your device could be infected with malware immediately and unbeknownst to you. Whenever possible, only click on website links that you trust. And be extra cautious when clicking on links in email messages.

10. Report cybersecurity issues.

If you are e victim of a cyberattack or see anything suspicious online, report it to the relevant authorities. This could be a phishing email, a malicious website, or any other type of fraudulent activity. By reporting it, you help prevent others from becoming victims of cybercrime.

Report cybersecurity incidents, threats, and vulnerabilities:

- UK: NCSC @ https://report.ncsc.gov.uk and submit through the appropriate channel(s)
- USA: NCCIC @ +1 (888) 282-0820 or https://www.us-cert.gov/report and forward phishing email messages and send suspicious/malicious website addresses to phishing-report@us-cert.gov
- Cybercrime is a serious threat. But, by following the ten above-mentioned security measures, you can significantly reduce the risk of you and others from becoming a victim and dramatically reduce hackers' returns on their time and effort investments. ■

BIO

Erik Alfonso Nilsen, PhD, is a physicist with advanced degrees in electrical engineering and mathematics. He has co-founded multiple companies since 2000, including TauTuk Cyber and Bio-Signal Technologies. Nilsen has a passion for signal/image/video processing, weak signal monitoring, analysis, and prediction, and has developed novel methods derived from chaos theory, fractal geometry, topology, electromagnetics, DSP, neuroscience, and nonlinear dynamics in his work. A strategic startup consultant for high-tech and med-tech startups, he also performs technology due diligence for PE/VC firms' portfolio companies. He is the author of numerous peer-reviewed publications in the physical and medical sciences, patents, and two books. Erik is a proponent of the decentralized internet and has recently been focused on out-of-band analogue and digital methods to help reduce hackers' success rates.

S & M victim = Cybersecurity victim!

Author: Sarb Sembhi

No! not that type of S&M, we mean Sales and Marketing. In a world where information and knowledge are growing faster than ever, we are not able to keep in touch with the latest developments of solutions and have to rely on trusted advisors, and when it comes to trusted advisors, security advisors come pretty high up. So, what’s wrong?

Once upon a time, security meant just security and those in the know knew what was what, because cyber security wasn’t even a thing then. But today, we work in an industry which uses one word in its phrase to differentiate it from when it was the only word used in the older industry (security vs. cyber security). But obviously there is more to it than just the one word.

I totally accept that there is a lot of sales and marketing which is, to some degree educational, which is one of the objectives of some sales and marketing. However, what if the person providing it doesn’t understand the technology but will be benefiting from the inaccurate education and knowledge they provide? Would we even know it? Should we be questioning everything our security advisor tells us?

I’m not suggesting that we don’t take advice from experts. But, for example, would I get a cybersecurity professional to advise me on where my alarm sensors should be in my house and install them? Absolutely not. A traditional alarm specialist has far more experience in understanding where the sensors should go than a cybersecurity professional. But then, would I get an alarm specialist to advise me on the most secure alarm system that is going to sit on my home or office network that I’m responsible for? Should I not want to know what network security knowledge they have, because the chances are I understand network security better than they do!

There has been a great convergence of technologies over the years and its coming to a bit of a head now in the sense that the technologies are getting infinitely great traction. The traction is that many manufacturers are developing and marketing systems which are easier and cheaper to install than their predecessors to some extent, but also these new products are providing instant control in the palm of your hand through connecting to

your mobile phone – without the need for dedicated TV screens or monitors (which we don't need, but still use).

The predicted invasion of IoT has been happening for several years, and no matter what you can think of, there are probably designs for that product or solution to be IoT enabled in one shape or form. It seems that any and every vendor out there has designs for giving us instant control of it on our mobiles.

The sales of network CCTV cameras around the world went up at the start of the pandemic, where a great majority of them were brought by small businesses; in particular, they were the ones which were the fastest to install and forget. So, it is no coincident, that not long after, several breach surveys and reports found that IoT devices were the targets of attack campaigns. Where they were targeting the communications of the devices in particular?

Well, how about that! You buy a security product to help you keep your business secure, but you have now let attackers from all around the world into your office and home, rather than just the local burglars to steal anything light and expensive. Who would have thought it?

What we forget, is that it was sold on quick and easy installation and access from your mobile device, it was not sold on how secure it was or with instructions on how to secure it effectively. – So, we all would have thought it would end in tears, but that is because we are in the industry.

BIO

Sarb Sembhi is CISM, CTO & CISO, Virtually Informed. As a well-respected industry veteran, Sarb speaks, writes and contributes to global security events and publications. He was the Workstream Lead for Thought Leadership of the UK Cyber Security Council Formation Project, is the Co-Vice Chair of the Smart Buildings Working Group and Executive Steering Board member of the IoT Security Foundation. He advises and sits on several start-up boards and is a Mentor on the Cylon accelerator programme. Sarb was shortlisted 5th in the IFSEC Global 2020 "20 Most Influential People in Cyber Security" and included in "2018 Tyto Tech 500 Power List" of influencers in the UK's technology sector.

Unfortunately, the full disclosure problem isn't just with security products like network CCTV cameras. A EU Data Protection Working Group wrote a guidance paper back in 2012 about IoT, and very wisely stated in no uncertain terms that its guidance was confined to personal consumer IoT items rather than other IoT products, as they recognised that the implications hadn't yet played out, just like the dangers of big tech having access to all your data hadn't played out while the GDPR was being written between 2008-2012. But we had a better idea by 2016 and more so by 2018, by which time the big tech had already won through their lobbyists.

Can we legislate out misleading marketing and sales about IoT products which don't inform us of vulnerabilities of the products? Well, we've had legislation around for food, cars, and several other markets, and over the last few years the EU and UK had agreed on legislation for IoT devices to adopt the top 3 of the 13 ETSI standard. Which for those of you who don't know, are now being included in the upcoming (it has been for over 3 years, but now bundled) Product Security and Telecommunications Infrastructure Bill.

This Bill doesn't affect any sales and marketing of any IoT security or any other products, but it does impose 3 basic measures that anyone providing the equipment must ensure (no default passwords, vulnerability disclosure and security updates). Will we see any more of this type of thing in the future? Will we ever be in a situation where security products like those that insurers expect us to have are actually cyber secure, rather than just physically burglar proof?

There are some countries like Singapore which have taken on not just the top 3 but all 13 of the ETSI standard's items as their minimum starting point for smart buildings (or connected places) technologies. Further, in the US the current President's "Executive Order on Improving the Nation's Cybersecurity" moves the whole discussion on in so many ways. Which although responds to attacks from nation states, does deal with attacks through IoT technologies as well.

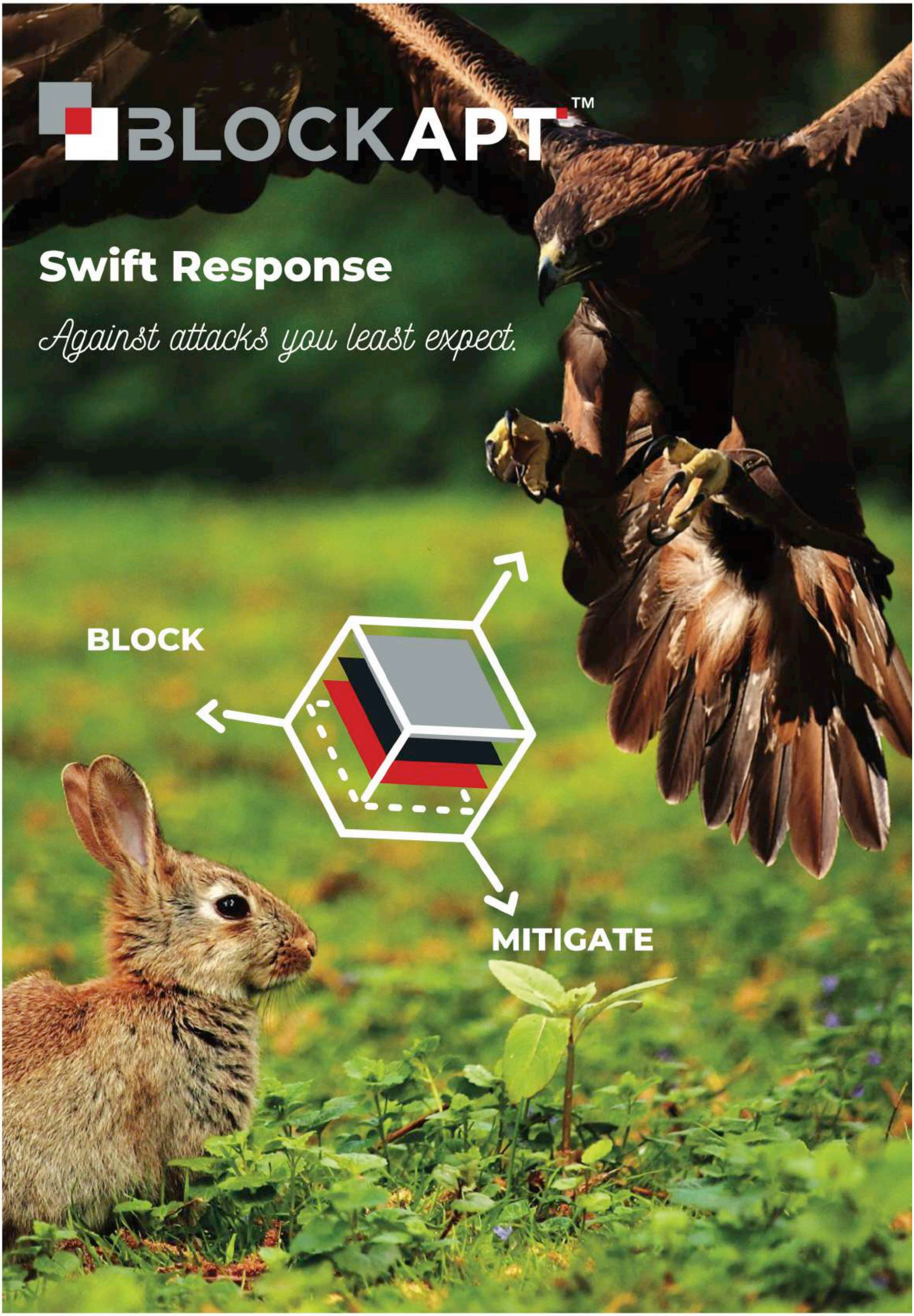
Right, that is all good for things not on the market today, what about the current sales and marketing of security products being sold by security experts today? The answer to that - due to the content of the new legislation containing the 3 items from the ETSI standard having been around for a few years, the respected industry bodies have responded in looking at the implications and the education that needs to go with it.

The various industry bodies for professional CCTV installation have created a Code of Practice (which will become mandatory at some point) that covers the cybersecurity of the product and the network installation part of it. It is a first step, but it is a very significant first step, and one that is also being considered by both the fire and lighting industry. What makes it significant is that there are similar network security issues involved in installing these solutions, furthermore the education they need and will be able to provide in the medium term is likely to be good and consistent.

Which all means that several industry bodies will be leading the charge on security through their members sales and marketing if all goes well. Which in turn means that there may be far fewer cybersecurity victims through bad sales and marketing (S&M) of some of these key security products. ■

If you are interested in the details of any of these issues, please do get in touch with me via my LinkedIn - https://www.linkedin.com/in/sarbsembhi/

BLOCKAPT™



Swift Response

Against attacks you least expect.

BLOCK

MITIGATE

See Yourself In Cyber: A world of opportunities and insight

See yourself in cyber: 5 practical steps to getting started.

Author: Segun Ebenezer Olaniyan

Cybersecurity is a career involving people, processes and technology to enable consistent operations that protect the confidentiality, integrity and availability of digital assets and information from intentional or accidental security threats.

With the evolution of Information and Communication Technology (ICT), cybersecurity has become essential as it helps protect communication and the exchange of information electronically. Due to the increase in internet penetration, cyber threats have skyrocketed leaving both individuals and organisations at the risk of cyber-attacks, hence the need for more competent and skilled cybersecurity practitioners.

BIO

Segun is an award-winning cybersecurity professional. He is the founder of Digital Security Village, an initiative with the goal of bridging the cybersecurity skills gap in Africa and beyond by equipping emerging cyber talent with the skills required for personal, business, and national security. Segun led the successful execution of a 6-hour, instructor-led Digital Investigation Bootcamp, which provided hundreds of cyber professionals from more than 15 nations across the globe with relevant digital forensics training. He is the founding partner of Cyber Safety Media, and the Lead Speaker at Cyber Safety Webinar. Segun is a sought-after presenter with global audiences and is an active author in his own right and contributor to cybersecurity periodicals.

The following are interesting facts about a cybersecurity career as enumerated by Flatiron School[1]:

- Cybersecurity is a rapidly expanding industry with a significant skills gap.
- Cybersecurity roles are high-paying and in-demand
- Many other technical fields have skills that can easily transfer to cybersecurity
- There are many paths to pursue based on your interests and skillset
- Soft skills like presentation, communication and collaboration skills are important in a cybersecurity career

Other interesting facts to know are:

- Anyone can start a career in cybersecurity with no or less technical experience
- Cybersecurity has a technical and non-technical aspect
- It is easy to carve a niche in cybersecurity due to the flexibility of the career
- Foundational knowledge is as important as advanced knowledge of the field (no jumping of classes, you must understand the basics)
- Cybersecurity can be combined with other disciplines (hybrid roles)

You can get into cyber security even if you don't have a cyber degree or backfround. Here's the complete guide for breaking into the cyber security industry.

5 practical steps to getting started in cyber

There is no one-size-fits-all approach to launching a career in cybersecurity, but there are various steps that anyone can take to get started. These practical steps include, but are not limited to:

1. Looking within:

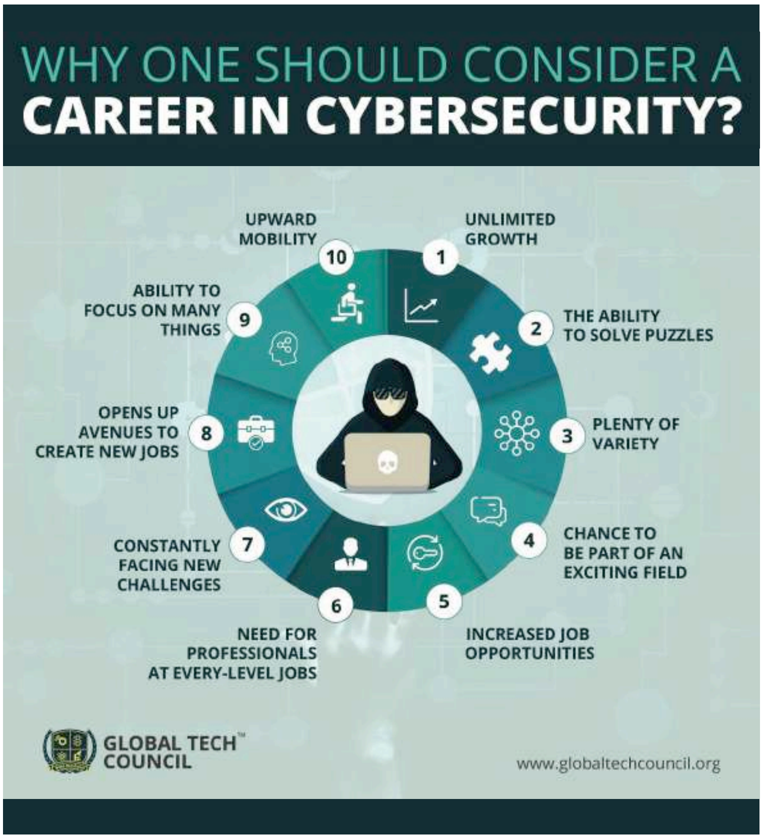
Due to how competitive the cybersecurity industry is, one must have the right intentions and motives for getting into cybersecurity. It is not enough to simply express your interest in this field; you must have a very genuine and impactful reason for your desire to begin a career in cybersecurity.

Thus, you must look within you and ask yourself a few questions. Your responses to those questions will serve as the foundation for your career. Your success in cybersecurity will be determined by your motivation for entering the field.

You need to ask yourself the following questions:

- What is my drive?
- Why cybersecurity?
- What innate abilities do I have that I can apply to this profession?
- What can I do differently in this profession?
- What can I contribute to the cybersecurity ecosystem?

It is insufficient to support your journey to a successful career in cybersecurity if all you want to do is start a job in cybersecurity because you need more money to pay your bills. You must examine yourself to see how you can have an impact on the cybersecurity ecosystem if you desire a successful career start and a long-lasting, meaningful career in cybersecurity.



WHY ONE SHOULD CONSIDER A CAREER IN CYBERSECURITY?

1 UNLIMITED GROWTH

2 THE ABILITY TO SOLVE PUZZLES

3 PLENTY OF VARIETY

4 CHANCE TO BE PART OF AN EXCITING FIELD

5 INCREASED JOB OPPORTUNITIES

6 NEED FOR PROFESSIONALS AT EVERY-LEVEL JOBS

7 CONSTANTLY FACING NEW CHALLENGES

8 OPENS UP AVENUES TO CREATE NEW JOBS

9 ABILITY TO FOCUS ON MANY THINGS

10 UPWARD MOBILITY

GLOBAL TECH™ COUNCIL

www.globaltechcouncil.org

2. Understand the basics:

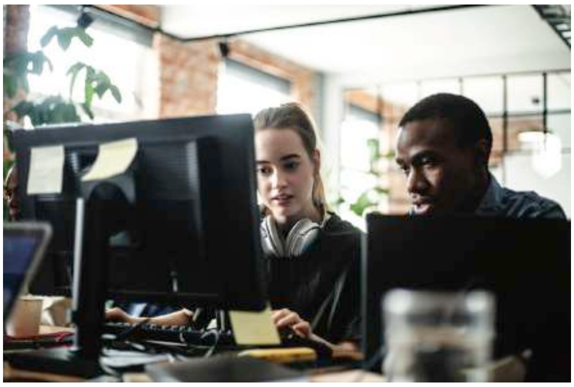
A basic understanding of IT and IT concepts is required to thrive in cybersecurity. Whatever path you choose and position you choose to follow, your basic knowledge and comprehension must be very solid, as they will most likely be assessed during interviews and will be necessary to complete your everyday obligations in your future role.

To thrive in cybersecurity, be sure to learn and sustain a basic understanding of the following:

- **Networking:** It is crucial to understand different network protocols, how the different network models work such as the OSI model, TCP/IP model etc., IP addressing and subnetting with the understanding of port numbers and the services running on those ports.
- **Operating System:** The basic understanding of the two major operating systems cannot be overemphasised – Windows and Linux. Understand basic Windows and Linux administration with file management, process management and how these operating systems log events.
- **Applications:** The basic understanding of a few applications like VPN, Database, firewall (both logical and physical) and other network applications like file transfer, SSH, E-mail etc., are necessary to start a career in cybersecurity because the advanced level challenges that come with these applications will require a basic understanding of how they function.
- **Programming/Scripting:** Understand the basics of HTML, Python, and Java; these programming languages will be required at one point or the other as you journey in your career to execute certain responsibilities in your role. The use of scripting, which includes languages like Python and Bash scripting, will enable you to automate some of the work associated with your role.
- **Framework, Standard and Regulation:** Understand the basics of the different cybersecurity frameworks, standards and regulations that exist. Know what each entails and what they aim to achieve. This understanding is crucial, especially for those interested in the non-technical aspect of cybersecurity such as Governance, Risk and Compliance (GRC).

3. Get work experience:

Cybersecurity is not an entry-level field, it is an advanced technical field with entry-level jobs, and these still require experience or a strong foundation[2]. You must focus on building sustainable skills that will make you stand out as an entry-level jobber or grant you the experience that will make you fit for entry-level roles.



You can start by setting up your home lab where you put to practice all that you are learning and then get hands-on practice experience using platforms like TryHackMe, HacktheBox, RangeForce, Cyber Ranges etc.

Apply for virtual internships on platforms such as Forage, Virtually Testing, Internshala etc. where you can engage real industry projects as replicated in various cybersecurity organisations and learn how to convert all these to a work experience.

4. Connect with the industry:

a. Get a mentor:

One of the great ways to connect with the industry is to get mentors in the industry. There are cybersecurity experts who understand the industry better and have sustained a certain level of experience in the industry that can guide you as you journey in your career.

Identify these experts on LinkedIn and connect with them. Your approach matters a lot; approach them with respect and let them see reasons why they should mentor you. Learn from their experiences, their mistakes and the strategies that help them succeed, and apply those strategies to your career.

b. Leverage LinkedIn:

LinkedIn is a social media platform for professionals with 810 million registered users and over 57 million registered companies[3]. On LinkedIn, there are many listings for cybersecurity jobs and companies. Also, recruiters, hiring managers and companies use LinkedIn to find suitable candidates.

Professionals can use LinkedIn as a virtual resume to show skills to the industry. Also, recruiters look at candidates' profiles on LinkedIn to see what they have been doing and their passion for the industry.

▸ **LinkedIn hack:**

- Have a well-optimised profile that will help you build a professional image for your cybersecurity career. This will help you stand out.
- Have a well-written CV or resume to send out for applications on LinkedIn with a custom cover letter written to fit each application
- Develop a social communication skill that will help secure a lasting network on LinkedIn
- Make strategic connections with relevant individuals or professionals and communities. Ensure that the majority of your connections are cybersecurity-oriented.

5. Contribute to the cybersecurity ecosystem:

Most hiring managers, recruiters, and organisations are on the lookout for individuals that have a passion for the industry and have made a consistent contribution to the cybersecurity ecosystem. The following are some of the ways to contribute to the industry and show recruiters and hiring managers how passionate you are about the industry:

▸ Start a blog where you can share your learning journey and contribute your quota to the field

▸ Partner with or contribute to cybersecurity projects to build a portfolio

▸ Derive a means to create cybersecurity awareness

▸ Create an avenue to help others grow while you grow

▸ Get your hands dirty during practical training and demonstrate it

Cybersecurity is a very competitive industry; hence a practical approach is required to sustain a great and rewarding career. You must be deliberate and consistent in your application of the helpful tips made in this article if you want to benefit the most from them.

All that remains is to wish you a successful and rewarding career in cybersecurity! ■

[1] How to Get into Cybersecurity, No Matter Your Experience Level. (2021, March 3). Flatiron School. https://flatironschool.com/blog/how-to-get-into-cyber-security/

[2] Davey, J. J. (2022, February 7). Entry into Cyber Blueprint. CMD | Knowledge Base. https://kb.cybermentordojo.com/knowledge-base/entry-to-cyber-blueprint/

[3] About Us. (2011). Linkedin.com; About Us. https://news.linkedin.com/about-us#statistics

The challenge that cannot be missed.

Author: Nicola Sotira

The business world is becoming more and more connected to the topic of digital. The digital transition is both a challenge and a symbol of economic recovery. However, adopting these new digital technologies exposes our society and businesses to more significant risks. These include the issue of cybersecurity along with sustainability issues. The business world must metabolise that cybersecurity is the new challenge of the digital revolution. The digital economy creates new contexts characterised by increasingly effective technologies that make companies, workers, and users hyper-connected while simultaneously increasing the chances of cyber threats.

BIO

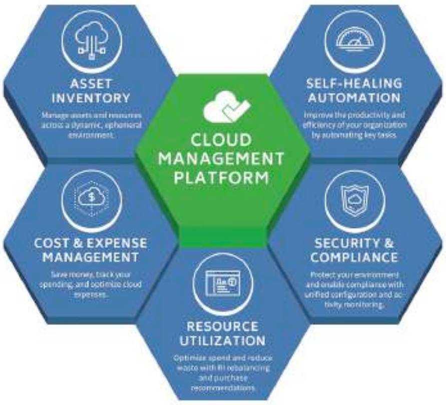
Head of CERT at Poste Italiane Group, Nicola has been working in the field of IT and network security for over twenty years, with experience gained in international environments. The contexts he has dealt with cover cryptography, infrastructure security, but also mobile networks and 3G. He has collaborated with several IT magazines as a journalist, contributing to the dissemination of knowledge related to security and its technical and legal aspects. Member of the Association for Computing Machinery (ACM) since 2004, Nicola has collaborated with several start-ups in Italy and abroad. In this field, he has participated with several companies in the design and development of mobile services; he is co-editor of the Italian version of Cybersecurity Trends (www.cybertrends.it) and has been on the board of the Global Cyber Security Foundation (GCSEC).

Consequently, there is a need to upgrade all actors involved in this supply chain to reduce and mitigate the possibility of cyber-attacks. In this scenario, strategies and investments in cybersecurity will play a crucial role in the ongoing process of digital transformation that companies and public administrations are facing. The common goal is to compete effectively in increasingly globalised markets where people, services, and products are hyper-connected. In addition, the work model is also evolving toward hybrid models with a consequent multiplication of devices connected to corporate resources.

The perimeter is no longer just that of our data center or corporate network but a more expansive boundary that considerably expands the possible attack surfaces. To ensure adequate governance of these issues, it will be crucial to have reasonable, flexible, and fully integrated solutions in digital processes because there will be no digital economy without adequate digital security. Let's consider what priorities we should guard in this economic and digital transition context.

Cloud asset management

Effectively managing resources in the cloud can provide visibility and complete control of all resources and infrastructure in our cloud environment. This is a crucial step toward a more secure and optimised infrastructure.


ASSET INVENTORY
Manage assets and resources across a dynamic, ephemeral environment.
SELF-HEALING AUTOMATION
Improve the productivity and efficiency of your organization by automating key tasks.
CLOUD MANAGEMENT PLATFORM
COST & EXPENSE MANAGEMENT
Save money, track your spending, and optimize cloud expenses.
SECURITY & COMPLIANCE
Protect your environment and enable compliance with unified configuration and activity monitoring.
RESOURCE UTILIZATION
Optimize spend and reduce waste with RI rebalancing and purchase recommendations.

The visibility must include a good view even in a multi-cloud environment ensuring smooth operation and real-time visibility of all our assets. Good management of this issue will give us greater visibility along with dynamicity in managing our inventory, allowing us to make thoughtful decisions about managing our assets. Using automated processing systems to manage asset discovery will reduce time-consuming data search processes by dramatically reducing human error in asset management by increasing accuracy in management processes.

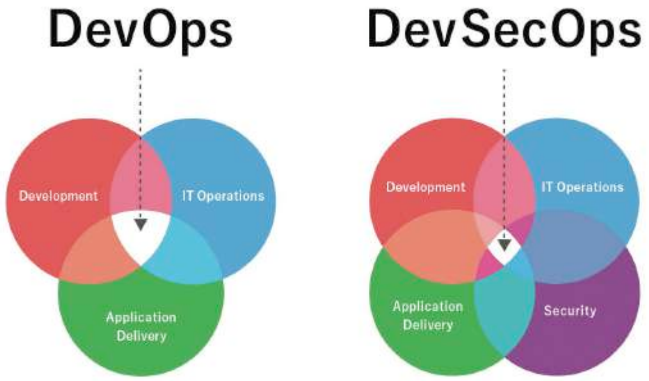
Automation in this area will consolidate and streamline security by ensuring we can keep track of security deployments and assess areas of risk and potential threats to our infrastructure. In this context, automated systems can flag and address vulnerabilities upon detection, thus ensuring that no critical security gaps remain. The issue of compliance can also be addressed in this area by identifying and making visible non-compliant assets. Since compliance will be one of the most important legal requirements in this area, the introduction of automation in asset management will ensure that we have strict checkpoints.

Dynamic risk

Risk management has shown in the recent period that adopting a dynamic approach is much more effective, thus reversing the traditional perspective. There is a need to analyse tasks, interactions, and operating modes to understand which elements actually lead to achieving business objectives and which generate dissimilarities, thus reducing risk factors. Fundamental to innovate in this area and develop a dynamic approach to risk management by changing the traditional corporate culture that must evolve from a reactive to a proactive logic. This means starting on a path that goes more and more into the area of data analysis, helping organisations map priorities and defining and orchestrate the action plans needed to best address each situation as it arises

DevSecOps

This acronym is becoming familiar and stands for integrating security into the application development cycle. This topic will become increasingly relevant, needs to be automated, and must be integrated into native development processes to facilitate the standard DevOps workflow and development. Artificial intelligence tools will be an enabler along with the automation processes of Application Security Testing platforms. Adopting automated analysis systems will enable incredible speed by making the development process and security testing at every stage smoother and more efficient.



Conclusion

It will be essential to preside over these issues by introducing the Digital Mindset, that is, having a predisposition and openness toward digital and how to use it. It means going beyond the simple technological tool and imagining the practical uses that can be made of it to succeed in achieving goals and results.

The challenge will have to be met by adding security at the speed of digital transformation and ensuring that it extends across every new internal digital process, external product, or business opportunity. The issue of cybersecurity is a responsibility that must be shared with the entire enterprise, as everyone will have a role in managing digital transformation and creating a secure ecosystem. ■

I need to be a tech wizard to work in cybersecurity. WRONG.

Author: Raj Meghani

Working in the world of all things cybersecurity is exciting, challenging and fascinating given the pace at which this sector is moving.

I'm passionate about what I do working in the cybersecurity space And YES – I didn't study IT related or technical/engineering courses for my Postgraduate and Master's degrees. I graduated in Marketing Management but over the last 25+ years I have been open to working a number of different roles in different industries – all of which have held me in good stead within my current role at BlockAPT.

BIO

Raj Meghani is Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. Raj is Editor for Cybersecurity Trends UK which has a global presence and is active in thought leadership and knowledge transfer of cybersecurity and business risk management.

LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/

Twitter: https://twitter.com/blockapt

Company website: https://www.blockapt.com

Let me explain. Working in cybersecurity is not just about technical skills. Yes – you need to have a good grasp on network systems and how they operate and communicate, understand software security and its implications, etc…

But it's also about problem solving and analysis. Any person that gets hacked or is a victim of cyber theft understands the RISK this poses to

them from a safety, reputational, credibility, financial perspective. Any business, irrespective of size, that gets breached or compromised will look at tightening their risk framework to mitigate against further reputational, legal, financial risks. Having a broad, diverse business background stands you in a good place to understand the IT/Infosec, operational, risk & compliance pain points of those looking to seek help from cybersecurity specialists. Cybersecurity is broader than just the IT division – its ramifications impact the whole business and its supply chain.

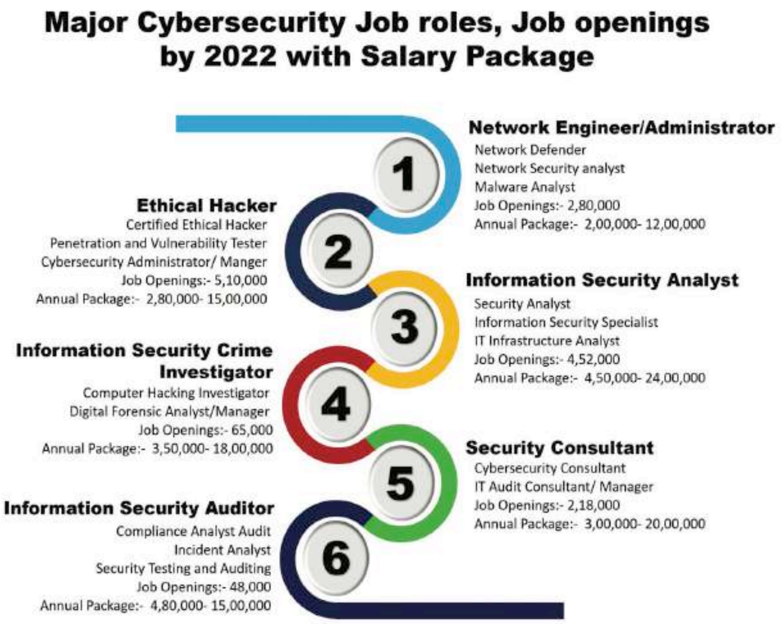
Am I a programmer or technical security architect? No. Do I understand end-to-end infrastructure, security & network operations, data security, encryption, security monitoring, vulnerability management, endpoint, email and web security, incident response management, etc what these attacks look like and who the potential threat vectors are? Yes.

Are you quick to adapt to a changing environment and flexible in your working style so you can think out of the box when the situation arises?

One of the communication skills I bring from my marketing and business background is the ability to translate and convey the technical aspects of cybersecurity into language that non-technical people can understand. It's called working in collaboration with the technical team, asking questions, challenging so you can resonate with whoever you are speaking to outside of the technical CISOs, CTOs, Security Architects, Security Analysts, etc.

There are a lot of cybersecurity materials, forums, videos, mentors/coaches who can help you get a foot in the door. You can study and top up your certifications, shadow someone who is willing to show you the ropes, attend free conferences and networking events (online and physical) which is a great starting point and so on.

Cybersecurity is an ever-changing world. So, if you are reluctant to change and don't embrace it, maybe working in cybersecurity is not the right path for you.



Major Cybersecurity Job roles, Job openings by 2022 with Salary Package

1 **Network Engineer/Administrator**
Network Defender
Network Security analyst
Malware Analyst
Job Openings:- 2,80,000
Annual Package:- 2,00,000- 12,00,000

2 **Ethical Hacker**
Certified Ethical Hacker
Penetration and Vulnerability Tester
Cybersecurity Administrator/ Manger
Job Openings:- 5,10,000
Annual Package:- 2,80,000- 15,00,000

3 **Information Security Analyst**
Security Analyst
Information Security Specialist
IT Infrastructure Analyst
Job Openings:- 4,52,000
Annual Package:- 4,50,000- 24,00,000

4 **Information Security Crime Investigator**
Computer Hacking Investigator
Digital Forensic Analyst/Manager
Job Openings:- 65,000
Annual Package:- 3,50,000- 18,00,000

5 **Security Consultant**
Cybersecurity Consultant
IT Audit Consultant/ Manager
Job Openings:- 2,18,000
Annual Package:- 3,00,000- 20,00,000

6 **Information Security Auditor**
Compliance Analyst Audit
Incident Analyst
Security Testing and Auditing
Job Openings:- 48,000
Annual Package:- 4,80,000- 15,00,000

If you are passionate, keen to learn every day, open to embracing new technologies and understanding what makes them click, inquisitive enough to seek out where the loopholes are to stay ahead of the hackers, brave enough to venture into a new industry which you know very little about, motivated by making a real difference to protecting people and businesses, high financial rewards, etc then enter the world of cybersecurity. You will shine, be rewarded on a number of different levels – and will never look back.

Let me leave you with a quote which resonates with me:

> ***"Security isn't something you buy, it's something you do, and it takes talented people to do it right."***

Take it from someone who's been there, done it and is still loving every minute of working in this space. ■

Cybersecurity from a governance perspective.

Author: Timo S. Koster

During my lifetime I went from a world without computers to ever present automation in our professional and private lives, on our desks, in our pockets, around our wrists and eventually in every device in our household.

This development brought unequaled opportunity and growth, at least for the roughly 50% of the world's population that has access to the internet. But it has also brought a sharp divide between the haves and the have nots, and a constant and increasing set of threats and challenges. Protecting our identity, our privacy, our data, our assets, is becoming increasingly difficult, just as it is difficult to decide who and what to rely on when it comes to protecting ourselves from online harm.

BIO

Timo S. Koster is a strategic advisor and board member. He was a career diplomat for the Netherlands for 30 years, with final assignments as Director Defense Policy at NATO in Brussels, and Cyber Ambassador for the Netherlands. He currently works for a number of clients in defense, security and cyber, including as Chief Strategy Officer for Quad9 DNS, a Swiss based non-profit.
Timo's Twitter: @tskos

Realistically, cybercrime pays, and state and non-state actors mostly get away with malicious behaviour. From a governance point of view, we face a set of challenges that are not easily tackled. And to complicate things further, with an ever-increasing speed of technology development we are shooting at a moving target. Keeping up with the evolving threats is a challenge in itself. Working in government, we concentrated on agreeing rules of the road in cyberspace, trying to catch the bad guys, and building cyber capacity in less developed countries.

It is important to acknowledge that whilst the Internet is universally recognised as part of our critical infrastructure, the ownership makes it different from, say, the public road, which is owned by the government that can decide on the maximum speed and other traffic rules.

But the internet is not, it is owned by everyone, which means the governance and management is shared between governments, private entities, tech platforms, civil society, and so on.

In other words, the rules of the road, the do's and don'ts, have to be established in dialogue between all these stakeholders. But where do they meet, do they speak the same language, do they share the same sense of responsibility?

So, the rules of the road of the internet are developing slowly, mostly on a voluntary basis, definitions of war, peace and crime are still relatively unclear. The discourse on this between all stakeholders is ongoing and reflects fundamental difference of world views, for example about the relationship between state and citizen. In the meantime, law and order is difficult to maintain.

And even if we do, if the state tries to enforce the rules, if social media take responsibility for the content on their platforms, imposing consequences on those who break the rules is not a given. States get away with cyber operations in other countries, online criminals have a low risk of getting caught, and private companies that abuse your personal data largely go unpunished. Discouraging (deterring) unwanted behavior seems far from effective.

We need far better situational awareness, for example through threat intelligence sharing between public and private entities, to facilitate attribution, and to enable decision making on what to do in response to transgressors. Public-Private cooperation in this area is far from perfect, and those in possession of threat intel are mostly focused on protecting the target rather than on identifying the culprit through sustained forensic work.

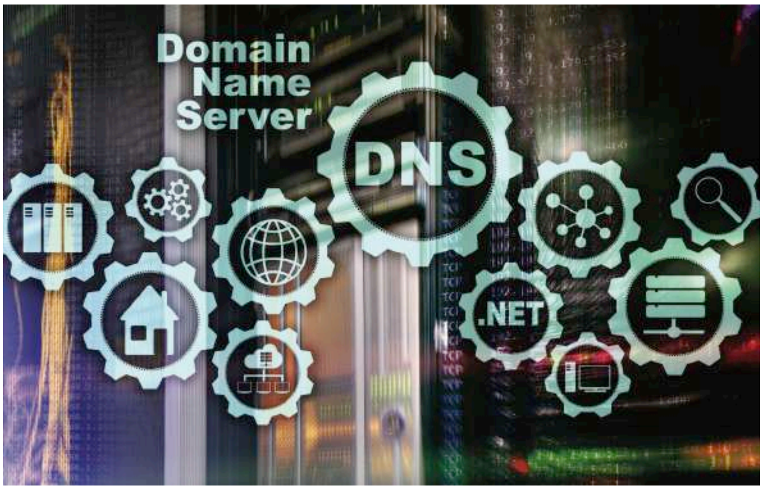
Apart from establishing the rules of the road in cyberspace, and raising the chance of catching the bad guys, governments have a clear responsibility to assist those nations that are less well equipped. A large number of nations are still not capable of protecting their critical infrastructure against cyber-attacks, giving their entire population access to a free and safe internet, affording them the opportunity to benefit from development, and protection of their human rights online. Cyber capacity building is therefore important and in our own interest; violations in our neighbour's cyberspace will almost certainly spill over into ours.

Global Commission on the
Stability of Cyberspace (GCSC)
Promoting Stability in Cyberspace to Build Peace and Prosperity

The United Nations have taken the lead in trying to close the digital divide, develop international norms for online behavior, and include cybersecurity into the so-called Sustainable Development Goals. But also, a project like the Global Commission on Stability of Cyberspace made an important contribution (www.cyberstability.org) This all sounds rather bureaucratic and political but is very much needed as one of the building blocks of a safe and free internet for all.

One thing is clear; the internet is a multi-stakeholder undertaking, and so is cybersecurity; governments, the private sector, civil society and academia must work much closer together, and it must be a combination of good governance and technical solutions.

After leaving government, I now work with a number of stakeholders who contribute in their own way to security and privacy online. Quad9 DNS for example is a recursive DNS resolver that combines a very high level of security with 100% privacy. This Swiss based non-profit offers a free DNS service around the world, protecting infrastructure, institutions and end users against all sorts of online harm. With server locations in about 100 countries Quad9 contributes to multi-layer protection for all, including in places where users are most vulnerable to online attacks from crime, spying and in some cases (their own) governments.



Being involved with this effort is very rewarding to pursue the goals that I worked on in government, as it allows me to bring together the technical, diplomatic and human rights communities and contribute to the universal cause of a safe and free internet for all. ■

Different voices, Different perspectives: Increasing diversity in security teams.

Author: Lisa Ventura

Diversity is defined as being the broad range of human differences, including but not limited to race, ethnicity, gender, age, sexual orientation, ability, and socio-economic status. Despite the benefits diversity can bring, many organisations have been slow to embrace it and to embrace the benefits that a diverse workforce can bring them. The cybersecurity profession in the UK faces specific issues in respect of increasing the pool of cybersecurity talent. These include supporting more neurodiverse candidates into the profession, increasing the number of women in the profession, and facilitating non-traditional routes into the profession.

BIO

Lisa Ventura is an award-winning cyber security awareness consultant, writer, and speaker. She is the Founder of Cyber Security Unity, a global community organisation that is dedicated to bringing individuals and companies together who actively work in cyber security to help combat the growing cyber threat. Lisa is also a mindset and mental health coach and offers help and support to those affected by stress, burnout, and mental health issues in cyber security and Infosec.

More information about Lisa can be found on www.lisaventura.co.uk; Lisa's twitter - @cybergeekgirl and @cybersecunity; Lisa's LinkedIn - https://www.linkedin.com/in/lisasventura/

The benefits of diverse teams in security:

Organisations should have a wide range of skills across their security teams, which is best achieved by increased diversity, and some important ways diversity benefits a team include:

1. Greater representation:

Representation in cybersecurity is essential, especially for teams to match the diversity of those who carry out cyber-attacks and to represent the groups they are protecting. If there is a lack of diversity this can lead to gaps in cybersecurity training due to assumptions in end-user knowledge. If you have a range of ages in teams, this results in a variety of valuable skill sets and perspectives, for example, cybersecurity professionals with long-term experience will have much more experience with malware, whereas those who are younger will be more versed in modern threats.

2. Variety of perspectives:

If you have people on your team from diverse backgrounds this will bring a variety of viewpoints, which means teams are more likely to get past obstacles and efficiently resolve issues by approaching them from different angles and viewpoints. Different questions may also be asked, and this level of diversity means teams are likely to have more options available to them and find better solutions.

3. Greater problem solving:

A diverse team will often provide more than just a range of different perspectives. When you are surrounded by peers who are more diverse, the members in the majority group may start to question their own assumptions, in turn helping them to improve their problem-solving capabilities. Visual diversity in teams often helps those involved to handle conflict in a more constructive way and in anticipation of potential conflicts are more likely to undertake more due diligence and research before presenting ideas, leading them to discover more problems on their own.

How to increase diversity

Increasing diversity can bring great benefits to organisations, but it does mean changing perceptions and examining any biases you might have. Some of the ways you can increase diversity in your organisation include:

1. Focus on staff retention as much as staff recruitment:
Studies show that up to 52% of women leave security careers, as do those with non-traditional backgrounds, and this is nearly double the percentage of men who leave cybersecurity careers. Some say this is because women don't enjoy their careers in security, but 80%+ of women in the industry say that they love their work. This implies that many from diverse backgrounds leave the industry due to culture.

2. Keep your conscious and unconscious biases in check:
Too often, we have a mental picture of what a security person is supposed to look like which does not reflect reality. Appearances can be very deceptive, so acknowledge that your biases may not be explicit or intentional and learn to recognise that they do exist. Listen to what people say, evaluate the work they produce and observe how they collaborate with others – these are all indicators of the value they bring to the organisation.

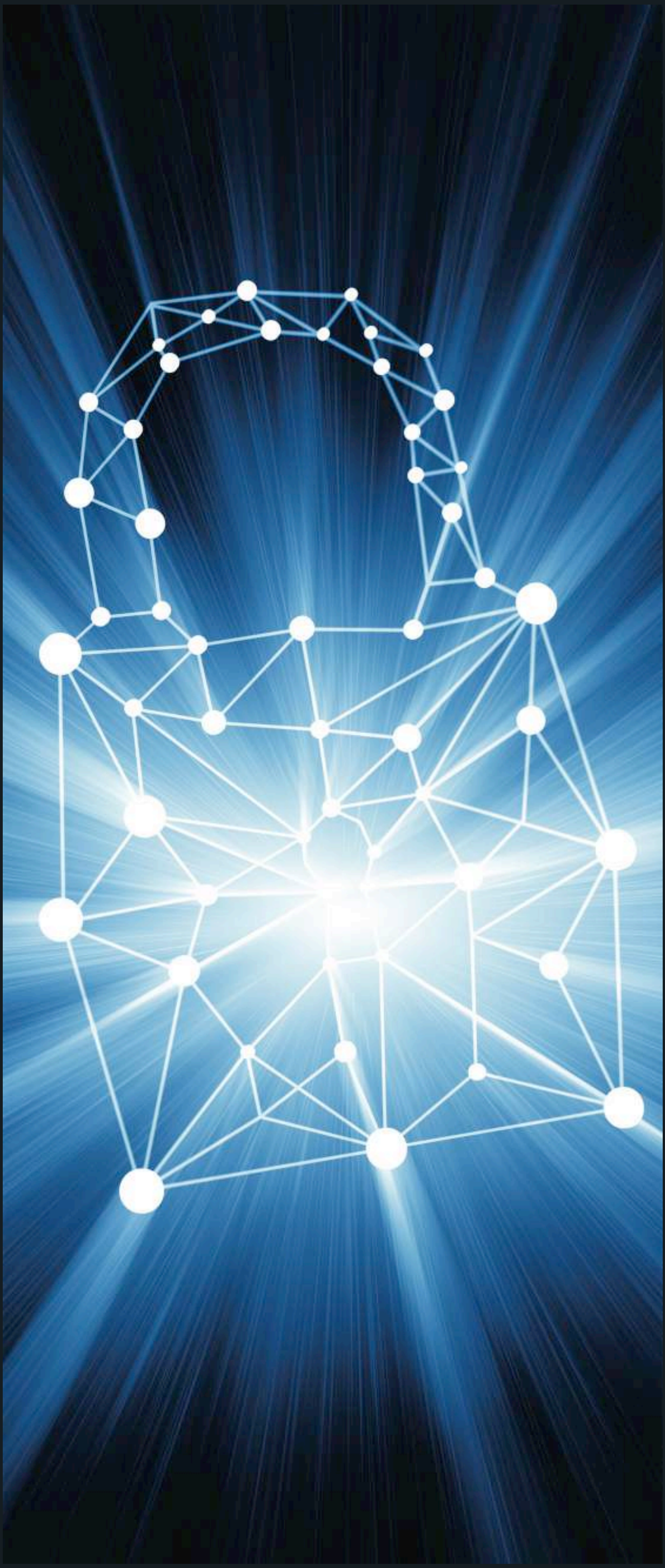
3. Nurture those who think uniquely:
Building a culture of inclusion where everyone has a chance to share their ideas can help hugely when it comes to improving diversity within security organisations. Not every idea will be a great one, but all ideas and opinions should be shared and listened to.

4. Increase your talent pool through flexible working:
Supporting flexible working hours, a flexible working location, job sharing or three weeks on/one week off enables people to set their own hours and location where they feel at their most productive, while still delivering on deadlines and projects. Trust that people can be productive even if they don't work in the same way or at the same time as others.

Final thoughts

To build a strong and diverse security team, you need to build an environment that supports and accepts differences of all kinds. Do not let bias about gender, the hours someone works, the location that someone works, or their appearance get in the way of nurturing all the great security talent available within organisations. Organisations should focus on creating security teams that mirror the make-up of their wider workforce. Only then do they stand a chance of warding off the growing cyber-threat. ■

Cybersecurity Trends



A publication

swiss webacademy
web for your business

edited by:

BLOCKAPT™

Redaction:
Laurent Chrzanovski and
Romulus Maier †
(all editions)

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
14 East Bay Lane,
The Press Centre, Here East,
London. E20 3BS
United Kingdom

www.swissacademy.eu
www.cybersecurity-dialogues.org
www.blockapt.com

BLOCKAPT™

BEST- Business Essentials Security Technologies

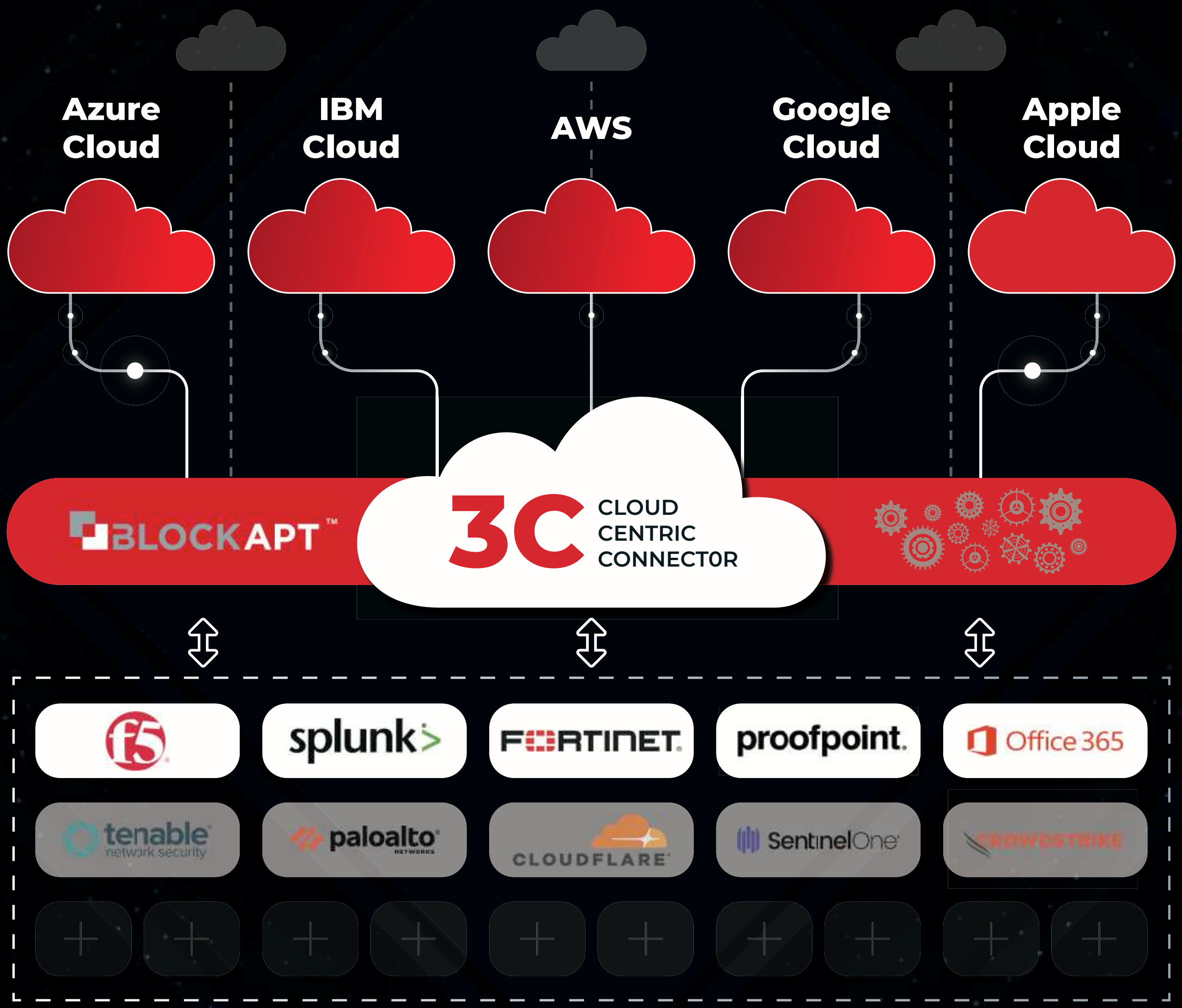
End-to-end protection across your business

- Endpoint Security
- Web Threat Protection
- Vulnerability Management
- Email Guard

blockapt.com

BLOCKAPT™

Centralised Cloud Management & Native Control



Azure Cloud

IBM Cloud

AWS

Google Cloud

Apple Cloud

- Seamless Orchestration
- Optimise your Cost & Efficiency
- Automated Config Management

blockapt.com