The Directors' Cut

Time to Think Differently About Cyber Security

Time to Think Differently About Cyber Security

Organisations must know and think like an attacker and observe their behaviours to become more cyber and business resilient.

'Think like the adversary – act like a hunter'.

Michael Jenkins MBE

As a Chief Information Security Officer (CISO) I have many tools at my disposal to help protect against cyber-crime and enable businesses to remain resilient to all manner of threats and risks – but probably the most important tool is to have a mindset that challenges the old notions of security, and instead align capabilities with the attacker's techniques and their intent in mind.

Future proofing for cyber resilience is of course key to reduce strategic business risk – if organisations want to get ahead of cybersecurity threats, or at least not carry critical risk, we need to start thinking about cyber security differently. One of the obvious ways is to take a page from cyber-criminals and learn from their behaviour, moving away from perimeter-based defence and into a data-centric one. Moreover, modern CISO's and cyber practitioners need to quell the old mantra's that still exist with a perimeter-based mindset and the old notions '*you can't do anything about the poor behaviour of end users*.' You can, but more importantly we should be implementing modern defensive instrumentation and counter-attack controls once a criminal has entered our networks. We should also be moving away from end user reliance in acting as our protectors – yes, collective defence is important, but of more importance is deploying capabilities that hinder, disrupt, contain, and make it more difficult for the criminal attackers once they're inside our environments. We can of course also invest further in our existing staff.[1]

[1] IT help desk = first line of defence, architects can be turned into security architects with some training and general IT practitioners can be turned into security-oriented IT practitioners who can organically spot and root out problems before they emerge. Organic security can be impressively effective.

Know your attackers

As a former bomb disposal officer and counter terrorist intelligence officer, I draw heavily on my previous experiences where, for obvious reasons, it was drilled into us to know your enemy, to know how they plan to attack you, to know their tactics, techniques, and procedures (TTP's) intimately. Then, and only then, could you use a smart approach to defend and deny their intent. I now spend a lot of time advising, mentoring, and coaching others on the cyber-criminal or the nation state attacker, much like a counter-intelligence officer would do - where cyber espionage takes place inside our digital environments. Criminals can invariably enter our environments with ease, they can and do remain there for long periods, scouting, recceing, planning, deploying their payloads to conduct nefarious activity. Most of the time without our knowledge. Many organisational leaders scratch their heads and are confused with the many conflicting pieces of advice on how best to protect their assets and their business – it's the noise, as many CISO's will tell you. Too much noise that mystifies a smart approach to the problem. One of the core starting points to think the journey through, is acknowledging that the criminal insider is more than likely already active within your business, amongst your data, living in your digital environment. Then you can think through the counter-tactics.

Learning from attackers

So, what can we learn from the criminals? First, cyber security is about more than protecting secrets or assets. For the future, it's about protecting our very way of life in today's modern world. Recent ransomware attacks across the globe and against academia in the UK have shown with clarity the devastating real-world consequences of cyber-attacks. When you look across the globe, many people are unaware from the media that whole towns and cities have been taken down through cyber-attacks in the last few years. In the USA alone, there were a number of such devastating attacks, including Baltimore and Atlanta during 2018-2020.[2] For the future, automation and scale are making the lives of cyber security defenders more difficult and much easier for criminals. They can automate attacks, as well as the tools they use to create attacks. So as ever, like a cat and mouse

[2] https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1?r=US&IR=T

game, its vital that businesses think ahead and predict the landscape and tactics of the attacker.

Perhaps one of my main focuses as a CISO is to ensure that outcomes are realised with investment, and that we look very hard at the return on security investment that considers not just how effective cyber security instrumentation prevents things from happening, but whether they will make decisions easier. We clearly need to not just invest in technology but in skills that will allow our institutions and businesses to become more resilient. We need to build a security culture where we care about our data, and take full advantage of simulated attack exercises, red team testing, threat hunting, and digital forensics and incident response. The old days of reliance purely on penetration testing are long gone – we need to ensure we do those but learn what the attacker does once inside our environments, and check often if they're there, and if they are, what they are doing. This is where most modern CISO's all agree – you have to continually monitor and hunt down the criminals to get ahead of the game, with skin in the game.

Staying ahead of the attacker

In the past, most organisations focused cybersecurity on the perimeter, and used passwords to authenticate users at the edge of systems, allowing them free reign once they got inside, the same thing happens now with network firewalls. This is often a dangerous way of continuing the status quo where criminals can enter through numerous gateways. It's like always looking at the doors, hatches, and windows, ignoring the internal landscape of an establishment where the crown jewels are. The smart, modern thinking practitioner obviously looks at a data-centric approach to security that protects their critical assets, high value intellectual property, and digital infrastructure which is now expanded and dispersed through the cloud to enable remote working.

Most organisations already have some sort of cyber security capability established, and it requires smart thinking and smart investment to go from that to truly future proofing a business with an assured cyber resilience regime. It becomes far easier when you can evidence through simulated attacks how criminals entered your environment, and how easy it was for them to conduct their attacks, exfiltrate data, encrypt data or deny you access to

your assets through sabotage of your infrastructure. If we can show the executive board that the assurances around business resilience are weak and make the argument that security investments protect the mission critical aspects of the business, and that the future proofing roadmap is smartly thought out, we can make a considerable difference to our communities.

Each business will of course have a different risk appetite, and differing business models with customers and partners who have an expectation of safe and secure IT operations and data management. The key is to ensure investment is balanced and proportionate, intelligence led, risk based, and vitally, it's interoperable to deliver the outcomes we desire. The modern CISO has many force multipliers including next generation instrumentation and artificial intelligence, Intrusion Detection Systems, Intrusion Prevention Systems, Defence in Depth, Active Defence, Red Teaming, Penetration Testing, Bug Bounties, and the like – but is it interoperable? Is it delivering outcomes and objectives that provide an evidenced ROI? Of course, no system will ever be fully secure, so the design of the infrastructure is important. Organisations should seek to stop the lateral movement of criminals once inside the environment, through network segregation, compartmentalisation, separating servers, networks, computers, and accounts that are outward facing and most vulnerable from systems, services and accounts dedicated to internal use, and containing key assets. It is inevitable that any organisation will be breached. The only question is 'what assets will be vulnerable when that happens?' Multi Factor Authentication (MFA) and meticulous Privileged Access Management (PAM) is vital as measures to hinder entry, stop lateral movement, and deny the escalation of access rights through stealing passwords to critical infrastructure systems.

Future proofing against attackers

Cyber detection is an arms race, fought between criminals who are forever developing more sophisticated TTPs, and security analysts charged with implementing defensive measures where they are needed most to contain an attack and mitigate the threats.

Simulated attacks and red teaming help assess the effectiveness of detection and containment instrumentation and processes, and vitally, such simulations clearly identify

where your weaknesses are from an adversarial POV. Run them once, remediate the issues, make a case for investment once you've shown how the attacker conducts the act, and then adjust, train, exercise, and test again against another attacker with different TTPs. All the time having quality monitoring instrumentation and ideally a threat hunting capability to keep on the front foot.

As with any defence against an attacker – exercising is crucial and it provides an opportunity to assess an existing capability and demonstrate its level of effectiveness, which in turn provides a level of assurance to executive stakeholders that is evidenced – where the assurance is low, you can begin to plug the gaps from the recommendations of the exercise. Examples are:

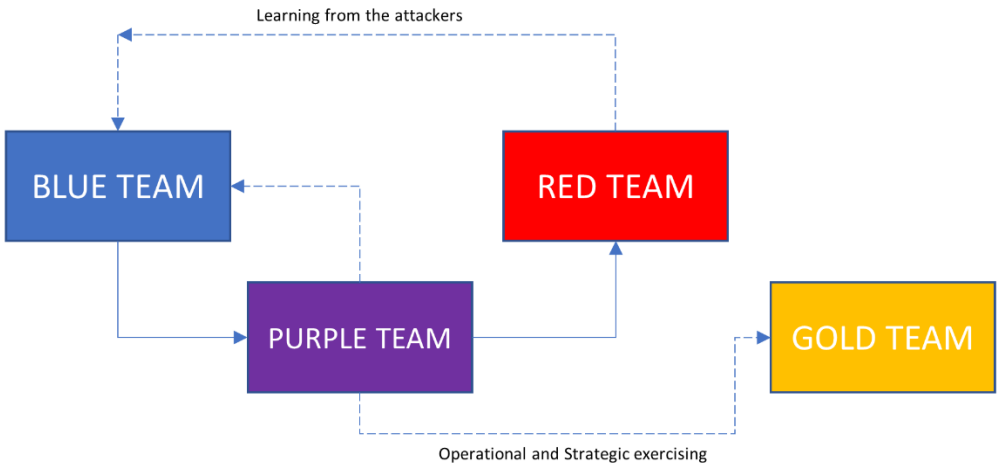
Blue team – The defender capability to detect, contain and mitigate an attack.

Red team – the team replicating the exact TTPs of a specific criminal attacker.

Purple team exercise – working with the red team attacker to learn from the way they attack us, seeing what we can detect and what we can't.

Red team exercise – Full simulation attack to test interoperable capabilities.

Gold team exercise – Full organisational cyber-attack exercise involving multiple senior executives for legal, comms, Data Protection, crisis response team etc.



So, in closing, where exactly do you get best bang for buck against a complex, modern, and highly evolving threat landscape? Well from my own simulated attack exercises and experience, the following capabilities are proving to be vital – but they must be implemented against a backdrop of efficient good practice such as patching, vulnerability management, hardening, safe configuration, 20 cyber controls, etc.

- MFA on all remote access, core systems, privileged users, high value systems and applications, core web applications – to hinder the criminal gaining access through stolen passwords or brute force attacks.
- Network segmentation and micro segmentation – to limit where the attacker can move laterally from system to system.
- Rigorous Privileged Access Management (PAM) – to hinder the criminal escalating their privileges to enter major infrastructure or services.
- Highly efficient disaster recovery capabilities and processes – to limit business damage and keep availability of data high.
- Moving towards Zero Trust concepts in a dispersed environment where access to data should be verified through identity, posture, and device checks.
- Cheap defence ensuring rigorous configuration of base systems (windows/linux/mac) Some online research will often save thousands of pounds!

As with any major programme and roadmap of capability development in the digital world, smart thinking, and smart investment to deliver the optimum outcomes remains the crux of the journey ahead – too much funding, time and effort can be wasted if the instrumentation and capabilities aren't thoroughly analysed at the very outset, thus avoiding a trajectory that will often lead to retrofits and too much costly deviation. But of course, don't forget to invest in our people - I`m often of the opinion that investing in staff through high quality training is vital to get the best out of expensive blinking boxes. Organisations are often very happy to spend millions buying latest and greatest AI-enabled products but their digital people are left behind without training budget for these products and, yes, certifications too.

Best of luck to everyone embarking on their new world of cyber resilience!

About the author

Mick Jenkins MBE

Chief Information Security Officer (CISO), Brunel University

Mick is Chief Information Security Officer at Brunel University. He is also a veteran army officer and soldier, mountaineer, explorer, and the author of four spy thrillers with a sprinkling of nation state cyber-crime. Follow him on Twitter @FailsafeQuery.

ucisa
Lumen House, Library Avenue,
Harwell Campus ,Didcot
OX11 0SG

www.ucisa.ac.uk

Administration: admin@ucisa.ac.uk
Events: events@ucisa.ac.uk

Registered Company No. 09349804