baesystems.com/unusualsuspects

The Unusual Suspects

BAE SYSTEMS

What's needed now, more than ever, is business **defence**

Introduction

Security used to be such a straightforward task for any business: lock the front door to secure your stock, and take the day's earnings to the bank.

That's no longer the case. The relentless march of information technology has created a dazzling, confusing plethora of problems, weaknesses, loopholes and complicated countermeasures. It can be daunting. It shouldn't be.

What's needed now, more than ever, is business defence.

We need to understand the threats and how they change, and employ the right people, processes and technology to counteract them.

It's far more involved. It's not for the faint hearted. But it is entirely achievable, and no-one should dread or fear it.

Business Defence needn't be excessively complicated, and it needn't be the preserve of the largest organisations. In fact, it can come down to knowing one's enemies.

If we can expose the shadowy criminals taking aim at our society each day, we can expose them to the cold light of day – and show them for what they ultimately are: fallible, understandable, human, and, ultimately, a threat that can be overcome.

Julian Cracknell, Managing Director, BAE Systems Applied Intelligence

The Mule

They've heard they can make thousands working from home. It sounds too good to be true – and it is. The Mule is part of a money laundering chain, cleaning stolen funds and goods for others.

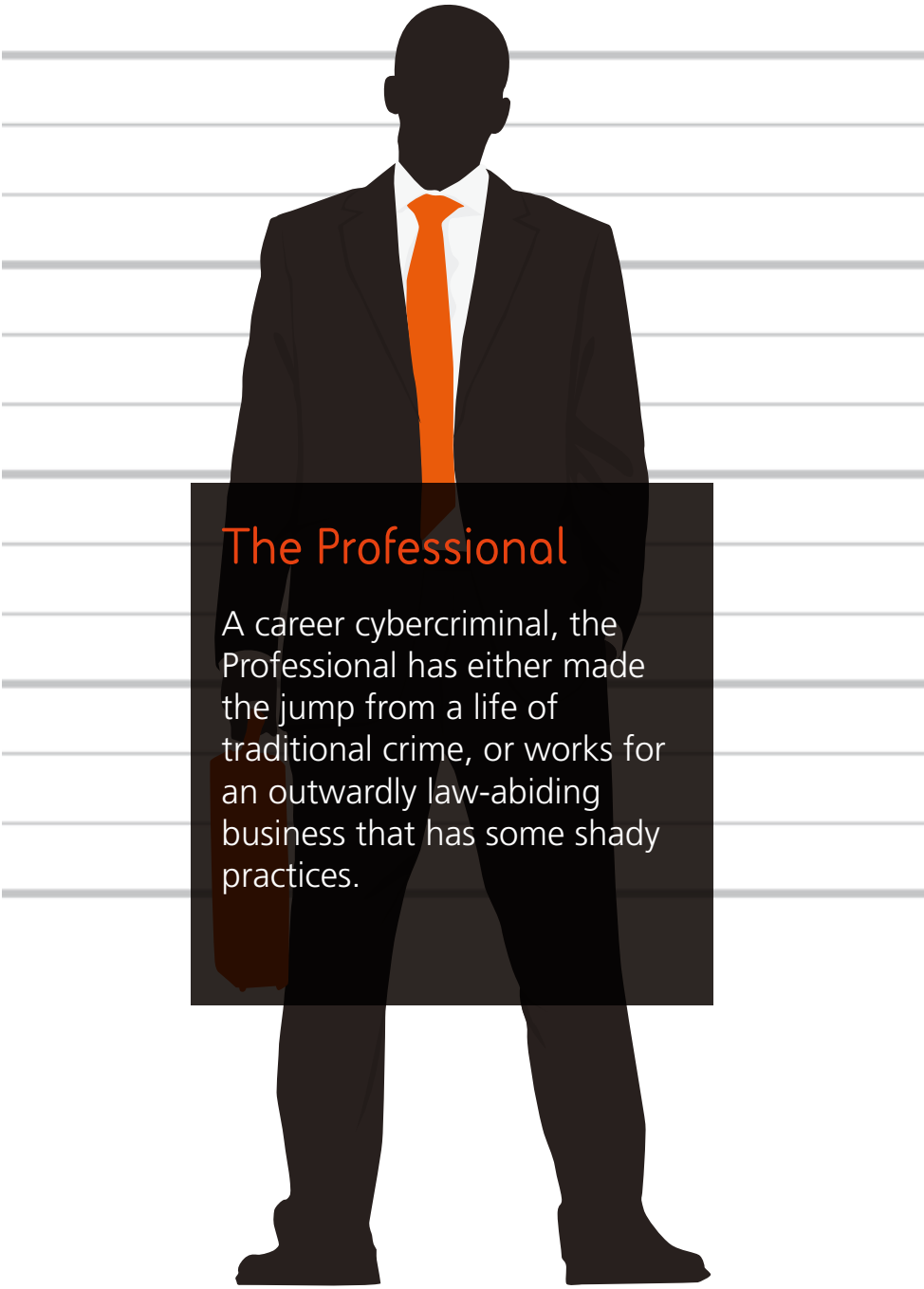
The Mule

The Mule is a casual criminal – or even a naive opportunist – used by others to launder the proceeds of cybercrime by taking stolen money and goods and turning them into 'clean' funds. They do this via internet payments, money transfers or online auctions. If the Mule starts out an innocent, they almost certainly don't stay that way - but fear or greed may well trap them for longer than they'd prefer.

They'll often be provided with training manuals by their employers that appear professional and legitimate and are assembled with a high degree of professionalism. As part of the joining process, they may also hand over all kinds of sensitive personal information, such as bank and passport details and their home address. Mules then receive payments in to their bank accounts, withdrawing cash and sending it on via money transfer. The Mule may also receive goods ordered with stolen credit card details, repackaging them and posting them onwards, to launder stolen payment card data into usable cash.

Mules are often motivated by greed or desperation, and work from home, internet cafés or free WiFi hotspots, relying on internet payment and bank accounts, as well as access to money transfer services in local shops. Mules run the highest chance of arrest or prosecution compared to other cyber criminal types, as their role is to provide the point at which virtual stolen goods are fenced or laundered into the physical world.

Once snared by a money laundering gang, Mules that perform well and prove to be loyal may be rewarded with 'promotion' and put in charge of managing their own team of mules. At this point, the Mule is likely to realise what they are into (if they hadn't already), and also likely to be 'in too deep' to make a clean break, either through simple greed or abject fear of the consequences.



The Professional

A career cybercriminal, the Professional has either made the jump from a life of traditional crime, or works for an outwardly law-abiding business that has some shady practices.

The Professional

The Professional works a 9-to-5 day at a company that might look like a legitimate operation. In reality, it's anything but: the Professional is engaged in cybercrime or cyber-enabled crime, running phone support scams, writing software for other criminals, or helping prop up the cybercrime supply chain.

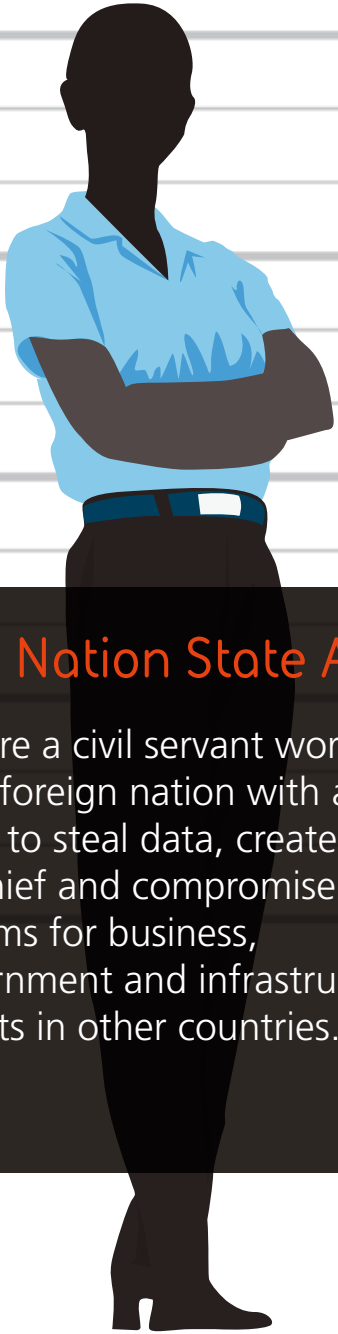
The Professional is a career cyber criminal who may well have made the jump from traditional organised crime into cyber-enabled fraud. They've got the skills and experience to evade detection and understand the structure of the organisations they break into.

An example of the Professional's work might include cold-calling members of the public under the pretence of technical support in order to persuade them to download malware. They're also likely to target people's PCs with malware via spam campaigns or 'malvertising' - online ads laced with malicious software.

Other professionals may be engaged in marketing these activities or parts of them in a 'Cybercrime as a Service' offering. This supports evidence that marketplaces for specialist cyber crime skills for organised criminals are well-established.

Professionals shy away from the riskier illegal pastimes – bank robbery, cheque fraud and the like – and instead use technology to lower their risk and exposure to the consequences. The Professional will have built up a solid reputation and a network of contacts, consultants and others, many of whom they've likely never met face-to-face.

It's entirely possible that more junior Professionals may start what they think is a legitimate job – for example as a social media specialist with foreign language skills – and find they are actually working for a criminal or nation-state backed criminal enterprise.



The Nation State Actor

They're a civil servant working for a foreign nation with a remit to steal data, create mischief and compromise systems for business, government and infrastructure targets in other countries.

The Nation State Actor

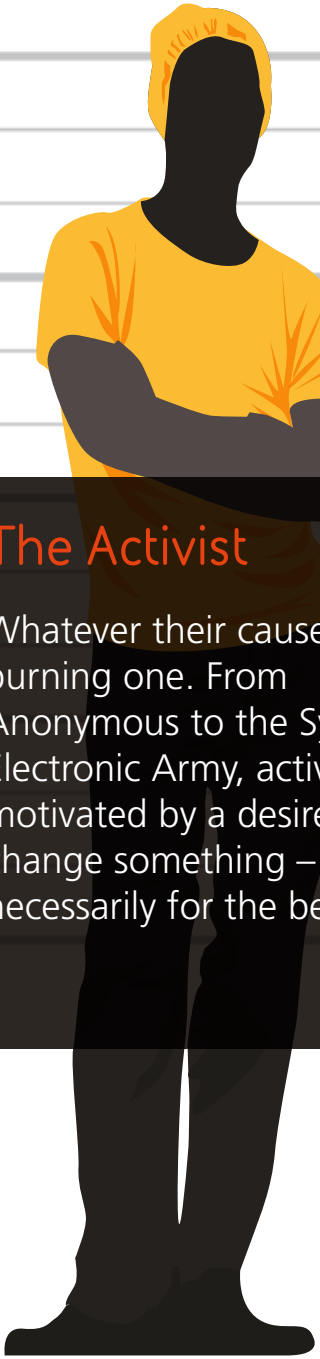
Nation State Actors work for a government to disrupt, steal from, or compromise target governments, organisations or individuals. They do this to gain access to valuable data or intelligence, and in doing so can create incidents that have international significance. They might be part of a semi-hidden 'cyber army' or 'hackers for hire' for companies that are aligned to the aims of a government or dictatorship.

The Nation State Actor knows exactly what they're getting into, and knows full well that the mayhem they're spreading overseas is tacitly supported by their state. They can work without fear of legal retribution – they will highly unlikely to be arrested in their home country for what they're doing. They often have close links to the military, intelligence or state control apparatus of their country, and a high degree of technical expertise.

Other Nation State Actor recruits may be picked for specific language, social media or cultural skills to engage in espionage, propaganda or disinformation campaigns. Nation State Actors also influence other Suspects, introducing new insights, tactics and attacks that are copied by others.

The Nation State Actor can be motivated by nationalism and tasked with gaining secrets from or disrupting other nations via cyber means. This isn't a task for the Getaway or the Activist – although both can easily end up being recruited, duped or coerced into acting on behalf of a nation state. Often, they operate covertly and almost never acknowledge ownership of their actions, unlike our other Suspects, for whom claiming credit can be part of the reward for their labours.

Nation-State Actors will go extreme lengths to cover their tracks, and to make it as difficult as possible for cyber security experts to trace their campaigns back to their country of origin – often planting 'false flags' to mislead attribution efforts.



The Activist

Whatever their cause, it's a burning one. From Anonymous to the Syrian Electronic Army, activists are motivated by a desire to change something – not necessarily for the better.

The Activist

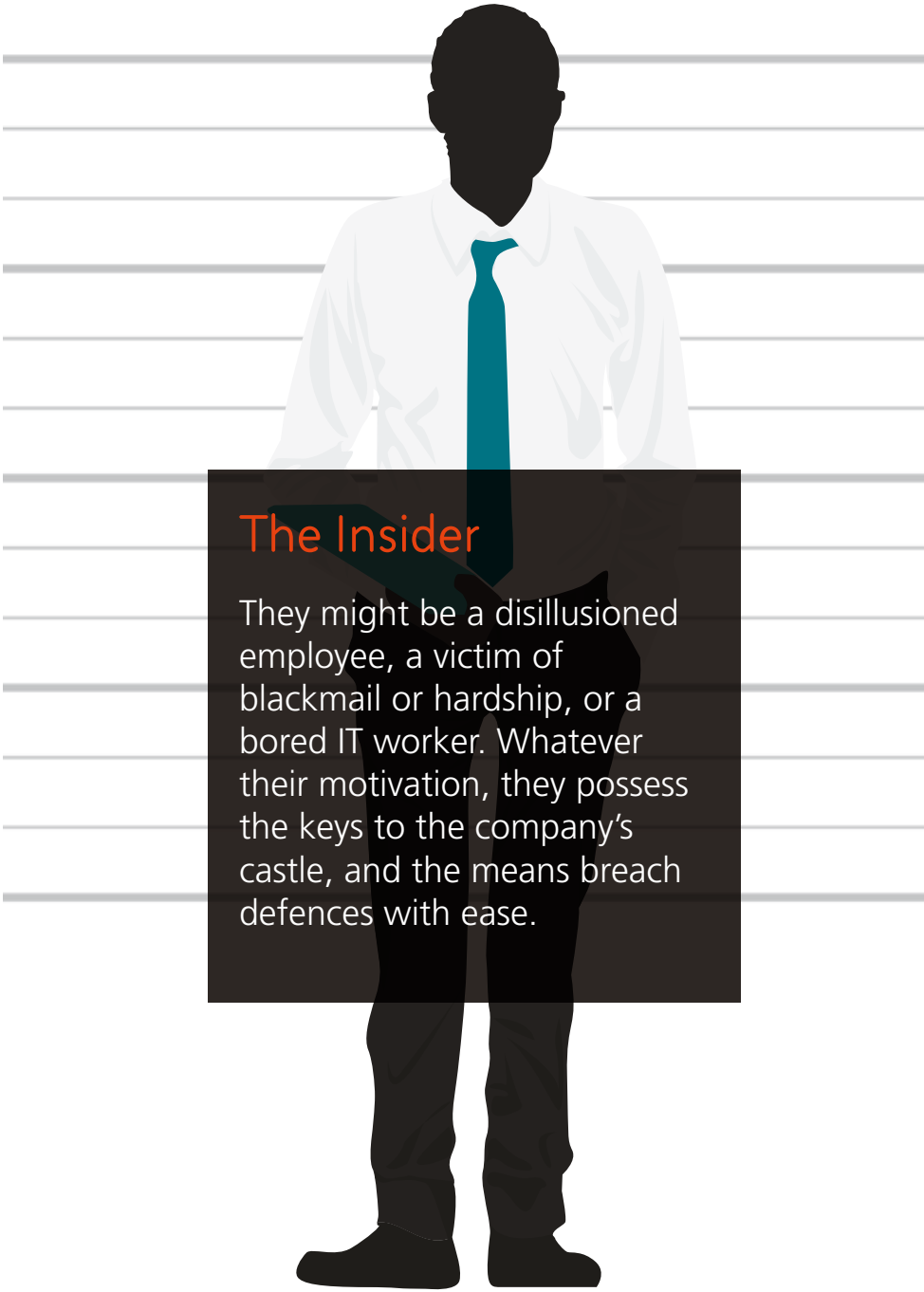
The Activist takes their political, religious or social cause outside the rule of law and onto the internet. They actively set out to target individuals or groups they disagree with using the power of the keyboard and the hacker's toolbox to harm reputations, steal data or target infrastructure. They're more likely to cause visible damage than to conduct their activities covertly.

The Activist's tactics can be crude and impulsive - but can also be singularly effective, and bring the age-old question of 'terrorist, or freedom fighter?' into the modern age. They may not have an 'A' grade in hacking, or be as organised as other attackers, but they can and will disrupt their targets' activities, discredit their operations and steal sensitive data to draw attention to or otherwise further their goals.

The Activist may turn out to be a common criminal, hiding their activity behind a popular cause. They can also provide a convenient 'false flag' for - or be a puppet of - more sophisticated actors, including nation state espionage groups.

The internet allows the Activist to cause trouble at a distance; they can then go public with a claim of responsibility at a time of their choosing to gain maximum media exposure. By operating under the banner of a collective such as Anonymous, and taking further steps to conceal their identity, the Activist protects him or herself from law enforcement.

The Activist's work costs money, and the way these threat actors are funded is often opaque and nuanced; very few receive a paycheque and funds for equipment and services direct from their sponsors. Instead, non-hierarchical arrangements with multiple sponsors who provide resources in exchange for expertise, project work and access to services allow the Activist to stay afloat.



The Insider

They might be a disillusioned employee, a victim of blackmail or hardship, or a bored IT worker. Whatever their motivation, they possess the keys to the company's castle, and the means breach defences with ease.

The Insider

The Insider comes in many guises: the disgruntled office worker, the blackmail victim in Accounts, the spy, the well-meaning innocent, or the small supplier with trusted access to your network. The Insider may conduct their activities on purpose, through carelessness, or through outside influence: falling for a scam or becoming the victim of blackmail, for example. This makes the Insider one of the hardest Suspects to anticipate and defend against. The Insider's position within an organisation can mean they can do just as much damage as the most sophisticated piece of malware.

Whatever their motivation, the Insider possesses the keys to the company's castle, and the means to breach or bypass defences with ease. Insiders have a variety of motivations; they may be complicit in the actions of other cyber criminals, but equally can be victims of blackmail, extortion or other threats to ensure their involvement. They're used to identify weaknesses in a company or organisation's security, or provide a route in via their own credentials.

Alternatively, Insiders may simply be a well-meaning individual trying to help what they think is a customer, colleague or partner out. The Well Intentioned Misguided Person (WIMP) – can be a significant danger to an organisation's security. They're often keen to help, expert at 'getting things done' and have a reputation within their organisation as the person others turn to to help solve tricky or seemingly insurmountable bureaucratic problems.

From mailing valuable documents outside the company (or moving them on thumb drives, mobile phones or via network backdoors, through to handing over login credentials), the Insider can bypass carefully-erected security and access controls. Disgruntled Insiders can leave a trail of destruction behind them – adding malicious code to company software, encrypting valuable files, or changing system configurations.

The Getaway

They've got youth on their side – even if they're caught, they're too young to go to prison. They're often manipulated and used by other criminals as proxies – and often end up taking the fall as a result.

The Getaway

Getaways have youth on their side. If caught, they're unlikely to get more than a slap on the wrist for their actions. Their hacking skills are generally basic, but Getaways are keen to impress their peers and will invest significant amounts of time in their dubious online activities, learning new skills and playing with the latest tools. On occasion, they can be used by other Suspects as proxies or diversions.

The urge to tinker, investigate, break and get one-up on authority figures are often key driving factors for Getaways. Even if their hacking skills are still a little basic, Getaways are often hard at work honing them. They see the challenge of breaking into systems and companies as a way to hone their abilities, impress peers and get noticed by the real 'Black Hat' hackers.

The Getaway's skills and aptitudes vary widely, from scripted attacks downloaded from the internet and used indiscriminately to sophisticated, targeted attacks aimed at achieving specific goals. Young cyber criminals often use a wide variety of skills. This includes social engineering – the ability charm, mislead and confuse people in person, over social networks or chat, or over the phone to extract information they need to break into networks. This approach requires no small amount of social aptitude, intelligence and wit.

Getaways are also influenced by other Unusual Suspects, such as the Professional, the Activist and the Nation State Actor, who may manipulate or recruit them to do their dirty work. Getaways can be used as a diversionary tactic by other cyber criminals, creating a smokescreen of small, obvious attacks to mislead or distract security teams and investigators.

Over time, they may also evolve into 'Professionals' or other Suspects, or turn to more legitimate employment where they can use their skills to a positive end.

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/5G

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai