RUSI Essay Prize

A resilient Critical National Infrastructure in the age of the "internet of things"

Stemming the 'Ripple Effect' of Insider Threat attacks on connected systems towards 2050

Introduction

Technological advances towards 2050 will lead to an increasingly connected, integrated and efficient world. The 'internet of things' will bring benefits in terms of national infrastructure such as community services, financial and infrastructure management, manufacturing and transportation. 'Smart cities' of the future will redefine users' relationship with technology and systems will evolve into something we cannot accurately predict today. However, recent years have highlighted the ability of malicious 'insiders' to conduct intelligent, complex and severe attacks on Critical National Infrastructure (CNI). We must let this be a warning sign and heed the lessons learnt, or else risk a 'ripple effect' turning into a 'tidal wave' of attack consequences as we accelerate into the connected world of the future.

The Interconnected World

Connectivity is the main focus for many technological advances in the modern world; from our home entertainment systems, to cloud computing and automated transportation systems. The so-called 'Internet of things' (or Internet of Everything), where numerous software and hardware components interact and interoperate within an internet infrastructure, is expected to consist of almost 50 billion objects by 2020 (reference 1). This approach is what is driving concepts such as 'smart cities', where the city of the future will have a 'transactional relationship with its citizens' through

more engaging, efficient and effective urban services that fuels sustainable economic development and provides an attractive environment for all (reference 2). A smart city is one that talks to itself; from monitoring traffic flow, controlling energy consumption, or even detecting when rubbish bins are full. While the applications are vast and varied, the simple concept of an interconnected world lies at the heart.

The CNI will inevitably be influenced and affected by these technological advances, mostly for the better. The opportunity for a connected network of communications, emergency, energy, financial and government services to better serve its citizens is clear. Many of the challenges that these areas face today such as information delays, lost records, over-bureaucratic processes and energy wastage, could be significantly improved through a 'smart grid' of interoperable parts. However, the very nature of what makes the interconnected CNI more efficient is also its inherent vulnerability to insider threat attacks. When attacks occur, they also have a greater potential to 'ripple' through the CNI network due to the numerous interlinked critical functions that may have to share the burden and suffer the consequences of malicious insider actions.

Insider Threats – an Increasing Risk

Insider threats are defined as attacks to an organisation or system from people within it; including employees, contractors, business partners, or anyone who has privileged access to or knowledge of systems, data, or practices (reference 3). They are often complex events, influenced by a number of psychological, political and socio-cultural drivers, which makes them hard to predict, identify and mitigate against. A holistic and proactive approach to insider threat protection is key to protect against the one

common denominator in all insider attacks; the human. It is also important to remember that whereas the human is always the perpetrator in an insider attack, they also often are the ones who spot an attack occurring. It is therefore essential to engage and involve workforces in insider threat identification and protection, as well as bearing in mind the attack potentially comes from within the same group of people.

Insider threats originate from four main sources:

- **Employees (managers)** – typically 'lone wolf' attacks motivated by long term financial gain. Their trusted position facilitates access to information and allows them to 'socially engineer' those around them to conceal their activities. Actions are harder to detect, last longer and generally have a larger financial impact;
- **Employees (non-managers)** – the most frequent and common source of insider attacks, although generally shorter, easier to detect and of lesser financial impact. These people are more susceptible to external coercion and are most often motivated by life pressures;
- **Business partners** – an increasingly common form of attack through trusted contractors or supply chains. These people are often afforded access without the same level of background checks as permanent employees. The attackers have a lower sense of loyalty to the organisation and are more susceptible to coercion or bribery (reference 3);
- **External coercion** – external groups such as organised crime networks, hacktivist groups, or national state actors may seek to bribe or coerce employees in exchange for information or actions. These groups will target

vulnerable individuals or those with an underlying incentive to attack the organisation (e.g. due to impending redundancy or perceived mistreatment).

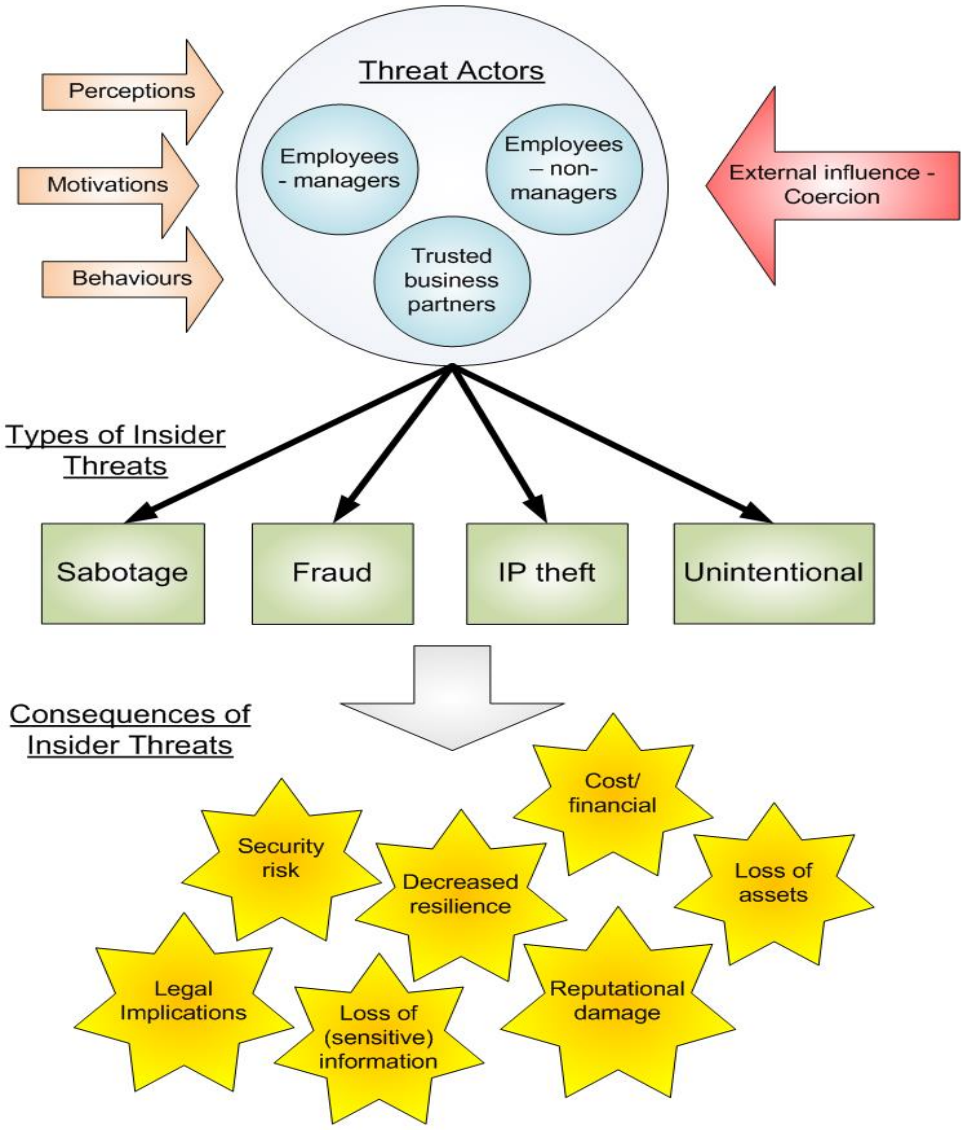
Insider threats take four main forms:

- **Sabotage** – an insider directs specific physical or electronic harm at an organisation or individual; such as deleting critical information, bringing down systems, or defacing public web sites;
- **Fraud** – an insider modifies or deletes an organisation's data for personal gain (financial), or theft of information, which leads to an identity crime (e.g. identity theft, sale of confidential information, or credit card fraud);
- **Intellectual Property (IP) theft** – an insider steals IP from the organisation, which can also include industrial espionage. This typically involves IP such as designs, formulas, source code and confidential customer information (reference 4);
- **Unintentional** – the actions of a person working within the organisation unintentionally and inadvertently harm its systems, processes and/or information. This is as a result of the organisation's lack of resilience to human error, rather than any underlying incentive amongst the workforce to conduct an attack. This can be referred to as the negligent insider, rather than the malicious insiders outlined above.

The consequences of insider attacks can be small or severe, depending on the ferocity of the attack and how early the actions are identified. The consequences can range from the obvious security risks and loss of information/ assets, to the crippling financial implications, to the less immediate but equally serious reputational damage.

Whereas the type and nature of insider threat attacks across various industries are different and varied in their methods and consequences, the basic human elements of motivation, mindset and behaviour remain remarkably similar. This is encouraging when we consider the resilient CNI of 2050; as we can confidently learn from contemporary and historic insider threat incidents and our knowledge of human insider threat behaviour, to start building and developing mitigation strategies and counter-insider threat measures today.

Figure1



Insider Threat Vulnerability

Interconnected systems are inherently more vulnerable to insider threats as the consequences will 'ripple' and amplify through a network after an attack has occurred. The relative damage that attacks cause becomes more severe and opportunities arise for multiple threat actors to attack various parts of the connected network to bring down critical functions. Insider attacks are becoming increasingly common in many industries; such as financial and economic services, defence and security and e-commerce; as those wanting to attack organisations see the insider route as the most viable, penetrable and damaging option. In addition to well known insiders such as Edward Snowden and Bradley Manning, there have been several recent high profile cases, including:

- Andreas Lubitz – the German Wings pilot who deliberately crashed a commercial airliner into the French Alps;
- Barclays Data Theft (2014) – insiders sold the details of over 27,000 customer files on the black market to be used for investment scams;
- Ashley Madison site – it is thought that insiders lead to the controversial website being attacked and sensitive customer details being leaked.

What is clear here is that insider attacks are not specific to any one industry and a neglect of the threat can lead to potentially catastrophic consequences. We will continue to see an increase in insider attacks until organisations and governments take it upon themselves to put more stringent and informed mitigations in place. Insider threat is often seen as the concern and interest of the academic community, as wider industry has been slow to adequately consider the risk. However, as more and more

insider attacks occur in different industries, the level of vulnerability will become clearer; opening the eyes of organisations themselves but also exposing their 'Achilles heel' to those motivated to attack them from within.

The Human Threat

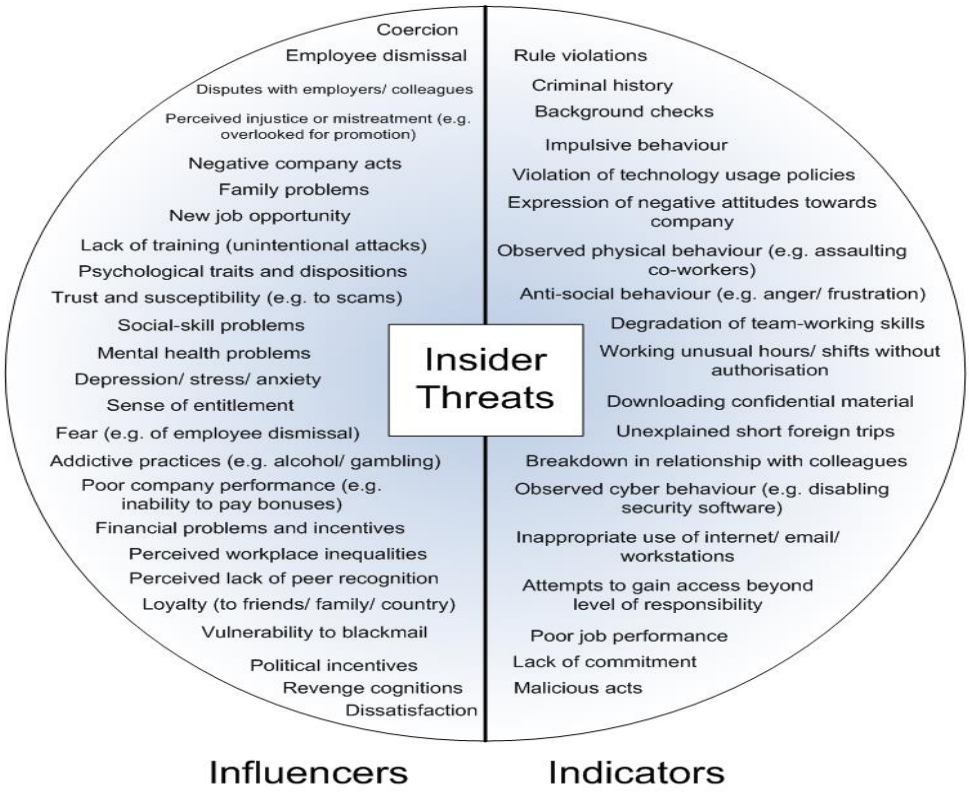
What differentiates insider attacks to many other threats to resilience is that human psychology lies at the heart of the problem. Understanding the perceptions and motivations of people within the organisation is a complex challenge, but one that must be addressed in order to safeguard the CNI. The human's role in delivering the critical functions of the future CNI is yet to be defined, especially as human input becomes less important as systems become increasingly connected and automated. There is likely to be a '**war of attrition'** between humans and technology, as humans seek to protect their jobs and responsibilities, while technology is gradually perceived to be a more reliable, efficient and resistant option.

What is vital is that organisations and technology developers over the coming years focus on maintaining and developing a healthy 'human-technology relationship'. Technology must exist as a method of serving and engaging the population, rather than replacing or superseding them. Indeed, it is often seen that organisations are overly-eager to fully automate, often overlooking the strengths and benefits of utilising their human capability. While machines may be more reliable, efficient and resistant to fatigue; humans are exceptional decision makers, problem solvers and able to process semantic and subjective information. There are exciting developments in the areas of artificial intelligence, unmanned systems and automated manufacturing, amongst others; all of which could contribute to a more efficient, reliable and resilient

CNI, but which also may trigger trepidation, resentment and even insider threat motivations amongst the human workforce.

When we look at the primary reasons for Insider Attacks today (as outlined in Figure 2 below), we see motivations such as terminated employment, disillusionment, perceived mistreatment, coercion and personal gain. There may also be a number of observable actions and indicators that can indicate insider threat intentions; such as rule violations, unusual work patterns and a breakdown in relations with colleagues. While the presence of any of these influencers or indicators in isolation is not indicative of an insider threat attack, when considered collectively they potentially become more sinister. All of these could be amplified as the human's role within the CNI is redefined. This could instil negative perceptions, beliefs and motivations within a number of 'threat actors', who wish to conduct malicious insider attacks.

Figure 2



It is absolutely essential that organisations consider two main aspects of the insider threat:

- The ‘routes to insider threat’ – how various influencers interact to affect the perceptions, motivations and behaviours of people within the organisation towards triggering conducting an attack;
- The ‘ripple effect’ of insider threat attacks – how attack consequences can ‘ripple’ and amplify through a connected network of components and at what speed and severity.

It is imperative to understand how insider threat motivations are formed, how the characteristics of the organisation and environment manifest these and the severity of such attacks should they occur. Organisations in the modern world invest heavily in technical systems and physical security, although the people within the trusted ‘inner circle’ are often over-looked and under-considered as a source of risk (e.g. once passing the initial vetting process). The problem becomes more severe as we move into a more interconnected world, where the relationship between humans and technology becomes more intrinsic and reliant and, therefore, a breakdown in either element results in more severe consequences.

CNI – Increased Vulnerability

CNI in 2015 is becoming more and more interconnected. Developments such as rapid manufacturing and network machinery, smart energy management and power generation systems and remote health monitoring and emergency notification systems are making critical functions more efficient and effective. Information is shared at ‘the touch of a button’ and systems are becoming more resilient to inevitable human

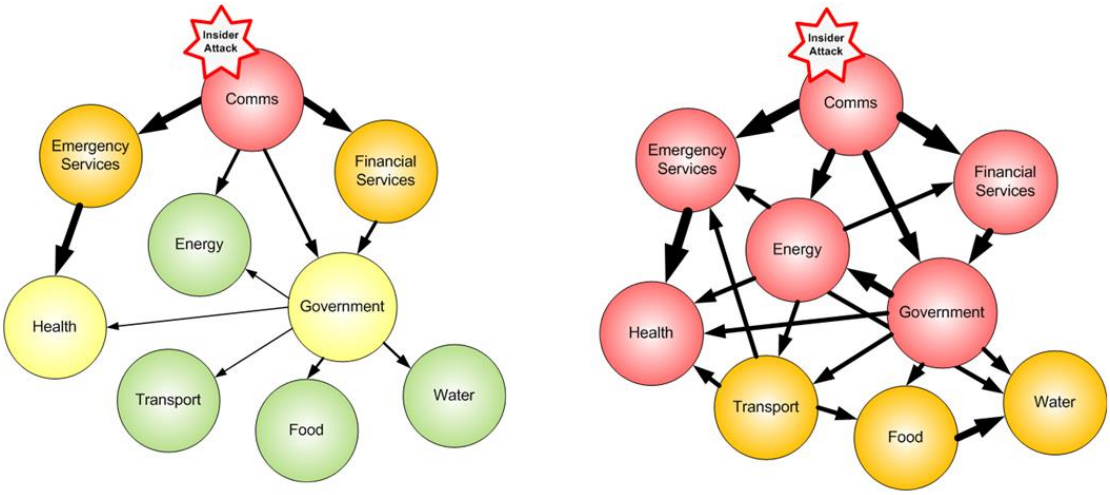
errors. While these are becoming increasingly common they are still often ‘stove piped’ by industry or application and are therefore resilient to damage or attacks to each other. For example, an attack on an energy network will not affect the emergency services and vice versa. However, attacks become far more of a concern when there are bridges between these areas, providing an inroad to amplify attacks to affect a far wider realm of systems and services.

The CNI of 2050 can be analogised as a spider’s web of strands and connections, which will ultimately lead to more efficient public services that better serve the population. Those areas currently independent of one another will soon be linked through numerous complex connections. While the ‘web’ will allow the different CNI elements to share benefits, information and resources, it will also mean that they will have to collectively share the burden of insider attacks. If an insider attack is the ‘fly stuck in the web’, then it soon becomes the concern of all the areas that are connected, rather than just the immediate locality. Some examples of future connected CNI systems include:

- Cloud and fog computing transportation systems within a city, at both the macro and micro level. This could be the fully automated control of an inter-city train network (macro), to numerous sensors within rail cars to aid in predictive maintenance and other actions (micro);
- Smart road networks and traffic lights sensing the proximity of emergency vehicles through cameras, weight and vibration sensors, to facilitate their safe and quick passage through a city; and

- Smart grids tracing energy consumption measured by smart meters; altering power consumption across various parts of an environment or urban settlement to increase sustainability.

Figure 3



CNI - 2015 CNI - 2050

As these CNI 'spider webs' are being developed towards 2050 it is essential that consideration is made to system and infrastructure design and development over the next 35 years. As mentioned earlier, an inevitability of the rapidly changing technological world is that humans can become increasingly suspicious and defensive in the face of technological advances that they perceive as their direct competition. Will the internet of things make current human roles redundant; such as emergency call handlers, control room operators and financial traders? In reality, technological advances generally do not lead to a reduction in the number of jobs, but a redefinition of roles within the organisation. Organisations need to pay close attention to using the human differently, not neglecting them entirely, or else risk developing a 'spider web' that alienates the very people they are intended to benefit.

Poor consideration of the humans within the organisation will lead to negative perceptions, beliefs and motivations building to a point where insider threats become a real risk. The best way to mitigate insider threats is to ensure that motivations for conducting them are not allowed to develop in the first place. The opportunity for any catalyst trigger events must be mitigated against and the organisational qualities that the people value must be safeguarded. People must be able to feel a sense of worth, belonging and ownership within an organisation; not be pushed aside into a passive role in favour of automated systems and processes. On saying this, while the human must stay involved, organisations must not become complacent with the privileges afforded to employees, especially those in more senior positions. Unrestricted access to information or a lack of supervision will allow those in positions of power to conduct more complex, concealed and severe insider attacks. The 'blind faith' of organisations in its perceived trusted employees is often their downfall in the face of insider threat attacks. Critical functions of the CNI must be tightly controlled and protected, with no single individual given total sole responsibility. Attackers in these senior positions are often able to conceal their activities for far longer, resulting in much more damaging consequences. This is a delicate balancing act; providing humans with ownership and responsibility, while not creating an oppressive 'big brother' environment.

A Holistic Approach to Insider Threat Resilience

As the CNI becomes ever more complex and interlinked within the Internet of Things then the challenge of safeguarding it in the face of insider threats becomes a greater task. Whereas solutions in the past may have relied solely on technical and/or physical protection, it is now clear that future resilience relies on a truly holistic approach. If

we are to build the resilience towards 2050 that can withstand a multitude of insider threats then there are a number of considerations that need to be made, including:

The Human Factors

Insider threat mitigation requires a human-centred approach to resilience and security. Organisations must focus their efforts on ensuring that the insider threat influencers (outlined in figure 2 above) are not allowed to manifest and where they are unavoidable that they are adequately dealt with. Mitigation of these aspects requires a joined-up approach between government, local management, support and technical teams within the CNI, as ultimately the insider threat should be the concern of all.

The following general guidelines, related to the human aspects, should be used to direct insider threat resilience efforts in an environment of the Internet of Things:

- **Know the enemy** – unsurprisingly, the first step in human-centred resilience requires an understanding of the people within and associated to the CNI. Organisations must monitor and control privileges and access to critical systems, monitor systems to detect suspicious behaviours and ensure that people are adequately supervised and interacted with so that disgruntlement and resentment can be spotted and dealt with early. Another critical aspect to mitigate the 'ripple effect' of insider attacks in the connected CNI is also to understand the relationships and interactions between personnel within different connected systems and organisations. In an environment of the Internet of Things there is a real danger that insider attacks may increasingly involve more than one threat actor, which makes them inherently more complex and severe. There is a risk that multiple threat actors could liaise together to conduct more complex, concealed and damaging attacks. By better

understanding the interactions and shared motivations of people across the CNI, organisations will be able to better identify sources of risk and where insiders could be collaborating in malicious activities.

- **Know the influencers** – insider threats are not a simple problem with a simple solution. While it is easy to attribute the blame to a single apparently obvious source, this is often only the 'straw that breaks the camel's back' and merely an observable result of a collection of contributing influencers. There are various situations, environments and events that may predispose or motivate a person into conducting an attack and it is essential that organisations are able to identify these areas of risk and intervene when they become apparent. These could include a wide variety of aspects; from mental health conditions, depression, family problems, financial struggles, political incentives, or motivation for revenge, to name a few. Understanding how the various influences combine to form motivations is probably the hardest challenge in insider threat mitigation and hence is not one to be neglected but rather to give additional focus. Over-focussing on the observable indicators or under-consideration of subtle psychological or socio-cultural aspects results in a warped and unrepresentative view of the problem. This will lead to organisations wasting time and effort in not tackling the issue at its genuine source. An increase in insider threat research in recent years is a welcome development, although any under-consideration of the 'human' influences to insider threat over the coming years will result in a CNI that is reactive to attacks and unable to proactively predict or identify its vulnerabilities. Organisations must begin to treat the insider threat with the same importance as is currently afforded to threats such as physical and cyber security, by

having structured programmes in place to monitor and track new and emerging influences.

- **Know the triggers** – understanding the various influencers to insider attacks is fundamental, although often an attack will not occur unless a trigger event, or catalyst, is present. Often, these can be events or actions 'in the moment', rather than any long-standing grievance. These could include events such as arguments with colleagues, disciplinary proceedings, redundancy, or substance abuse. CNI organisations must ensure that their workforce is surrounded by a safe and supportive environment that limits the potential for trigger events. In the future, it must also be remembered that trigger and catalyst events seemingly unrelated and removed from the organisation may well affect it, due to the increased interconnectivity and 'ripple effect'. It is more likely that wider social, cultural, political and environmental effects could permeate into organisations unresilient to their influence, instilling insider threat motivations or even triggering an attack into occurring.
- **Know the 'routes to insider threat'** – Understanding the 'routes' refers to being aware of how the various influencers and triggers to insider threat interact and combine to initiate malicious behaviour within the threat actor. This is essentially the 'final part in the jigsaw' in understanding the human factors to insider threat. While no understanding can be anywhere near 'bullet proof'; as we are dealing with the fundamentally unpredictable nature of human psychology; getting to a point where influencers and triggers can be identified and predicted within the workforce allows for an As Low As Reasonably Practicable (ALARP) approach to risk mitigation, which must be

a central aim for the future CNI in the face of a growing and evolving insider threat.

Consideration of the complex psychological, socio-cultural, environmental and situational influencers and how they interact to instil insider threat motivations and behaviours is the key to effective mitigation. Mitigation and intervention measures must be actively implemented to ensure that 'routes to insider threat' are not allowed to develop or infiltrate elements of the CNI network.

The Technical Vulnerabilities

The vulnerabilities of the technical elements of the CNI are harder to predict at this stage, as new technologies and systems are still in development, or have yet to come to light. What we can confidently assume though is that humans will retain a large degree of interest and involvement in whatever these technical elements will be. It is for that reason that we can also assume that insider attacks will continue to present a great risk to resilience in the connected CNI of the future.

It is important that within the 'spider web' CNI of the future that we adequately understand where the critical functions and systems lie. However, with such a myriad of strands and connections this poses a significant challenge. So many 'bridges' between the different systems and assets requires the development and implementation of many more 'gates' to attempt to stem the flow of insider attacks rippling through the network. The challenge here is to implement effective protection measures, while ensuring that the CNI connectivity remains unaffected as it is these shared points between the disparate elements that constitute the essence of the Internet of Things. What must be remembered is that insiders are much more likely to go 'straight for the kill'; targeting those critical systems and functions rather than the

peripheral secondary elements. Understanding of such critical vulnerability is therefore the fundamental 'first step' in insider threat mitigation.

As well as protecting technical systems against malicious insider attacks, there is also a third emerging type of threat; a hybrid of negligent and malicious insider; that is called the 'compromised insider'. A compromised insider is someone whose access credentials or computer have been compromised by an outside attacker (reference 5), typically through actions such as malware attacks or scam phishing emails. As the world becomes increasingly connected, the cyber environment becomes more sophisticated and cybercrime groups become more numerous and intelligent, the risk of compromised insiders increases dramatically. In addition, the very nature of the CNI makes it a prime target for malignant outside attackers; as it provides the opportunity to seize sensitive information and IP, trade secrets and personally identifiable information. It also presents the opportunity to disrupt or destroy assets and systems that could have a crippling effect on security, economy, public health, or safety. A compromised insider is evidently not someone who intends to harm the organisation, but someone who uses technical systems that are not robust or resilient enough to protect them from unwillingly becoming the victim of outside attackers. Clearly then, this is a technical vulnerability rather than a human fallibility, although interventions such as training and awareness campaigns can increase the vigilance of the workforce against such attacks.

Developing Insider Threat Management Programmes

There are many lessons we can learn today to help inform our long term strategy for CNI insider threat resilience and security, although we must begin with some short-

term ‘quick wins’. The best way for CNI organisations today to future-proof themselves against both the current and future insider threat is to develop and implement insider threat management programmes. Indeed, some organisations are much further ahead than others in this respect; the US Government rolled out a National Insider Threat Policy (reference 6) in 2012, which mandates that all government departments develop an executive branch programme for the deterrence, detection and mitigation of insider threats. This is a welcome forward step in the counter-insider threat challenge and will hopefully set precedence for other governments and industries.

Governments and industry within the CNI should be actively looking to establish insider threat management plans, teams and programmes that take a holistic approach to the problem; considering both the human and technical elements as outlined in this article. A few key steps in the development of insider threat programmes include:

1. **Gain leadership support** – programmes must have support within the higher echelons or governments/ organisations;
2. **Conduct Insider Threat Audit** – conduct investigative and analysis activities to build an understanding of the workforce, the environment and the threats;
3. **Create the insider threat management team** – engage personnel within disparate teams and divisions; including technical, support and leadership areas;

- **Identify and Utilise the Latest Technology** – technology plays an integral part in the success of a robust insider threat programme. Insider threat detection technology should focus on behaviour, not devices (reference 7);

- **Continuous Risk Management** – seek to continually track and monitor assets, points of vulnerability, high-risk positions and threats (reference 8);
- **Establish Formal Processes** – insider threat management must be underpinned by formal structured activities to ensure that it remains at the forefront of the organisation's resilience strategy;
- **Communicate with and Engage the Workforce** – the workforce must be communicated with and engaged in the programme as much as possible (e.g. training and awareness campaigns). As mentioned earlier, even though the threat resides in this group it is the same people who are best placed to identify and mitigate emerging threats;
- **Maintain and Build the Insider Threat Community** – the programme must ensure that a community of individuals combating the insider threat is maintained and supported across a number of different areas within the organisation. Insider threat must be treated as an on-going concern.

Into the Future…

The insider threat has risen to prominence in recent years and will continue to pose a real danger to CNI resilience towards 2050. Government and industry must learn lessons from today to mitigate the threat of tomorrow. The insider threat is likely to become more of a severe danger as the connected CNI of the future, underpinned by the Internet of Things, presents more potential vulnerabilities and provides the opportunity for attacks to 'ripple' through the network resulting in a 'tidal wave' of consequences.

Resilience and security must adopt a human-centred approach to attempt to mitigate the development of insider threat motivations and limit the consequences of attacks

should they occur. Some governments and industries are making proactive steps; although as a whole progress is too slow. The insider threat will continue to evolve into a larger, more intelligent, more complex and more concealed enemy, to which we must not expose the 'weak underbelly' of the CNI.

References

1 – Cisco Internet Business Solutions Group, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, (Cisco, April 2011), p.3.

2 – UK Government, 'Smart Cities Background Paper', Department for Business Innovation and Skills, 2013.

3 – CERT (Carnegie Mellon University), 'The CERT Guide to Insider Threats – How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Software Engineering Institute Series, 2014.

4 – CERT (Carnegie Mellon University), 'Common Sense Guide to Mitigating Insider Threats 4th Edition', Software Engineering Institute Series, 2012.

5 – Mike Potts, *Combating Insider Threat* (Lancope, 2015).

6 – US Government – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 21 November 2012.

7 – Lockheed Martin Corporation, *5 Steps to Develop a Successful Insider Threat Detection Programme,* (Lockheed Martin, 2015)

8 – Dawn Cappelli, 'What a Relief – It Works! How to Build an Insider Threat Program in 1 Year', paper presented to RSA Conference, San Francisco, April 2015