A HOLISTIC REVIEW OF CYBER RISK FOR THE DISTRIBUTION OF POWER

Steve LITTLE
Frazer-Nash Consultancy Ltd – UK
s.little@fnc.co.uk

Anuj NAYYAR
Frazer-Nash Consultancy Ltd – UK
a.nayyar@fnc.co.uk

David NEILSON
SP EnergyNetworks - UK
david.neilson@spenergynetworks.co.uk

ABSTRACT

This paper presents the requirement to consider cyber risks holistically across a complex environment, such as the distribution of power. Organisations typically use technology as a prevention against a cyber-attack. Organisations are more than just technology they comprise of people, processes, information, technology and facilities. Technology has its place in protecting an organisation against a cyber-attack or to enable it to recover, however it is not the complete answer. For an effective defence, or to recover, from a cyber-attack organisations need to understand the importance of people, processes, information, technology and facilities and their interdependencies.

INTRODUCTION

Critical National Infrastructure (CNI) comprises of services required to keep a society and its economy functioning, this includes electricity generation, transmission and distribution. With the increasing demands of modern and disruptive technology, the distribution of reliable, regular and efficient electricity is essential, with the distribution of electric power being the final stage, and arguably the least resilient, delivering electricity to commercial and residential customers.

Given the changing profile for the generation and distribution of electricity across today's society, and the extra responsibilities of a Distribution System Operators (DSOs) over the traditional Distribution Network Operators (DNOs) model, they are particularly vulnerable and an obvious target from many different cyber aggressors, including nation states, cyber criminals, script kiddies or insiders. The 2013 film by National Geographic, American Blackout, dramatizes the effect of a cyber-attack to power distribution in the US. A coherent and consistent cyber-attack on the distribution network for power, will have a long lasting and profound affect, particularly given the fast paced and disruptive developments around digitalization. Given the extremisms in American Blackout, regulatory incentives were not necessary a consideration. Unlike traditional conflict zones, most governments do not see themselves taking the lead in national cyber defence, it is seen as the responsibility of the private sector. However, UK DNOs are financially incentivised to improve level of performance, minimise customer interruptions and customer minutes lost. How well prepared are DSOs or DNOs prepared for a catastrophic cyber event such as that depicted in American Blackout?

The distribution of power is highly complex, involving an amalgam of:
People, Processes, Information, Technology and Facilities (PPITF). Within any organisation, including those of a DSO, an understanding of PPITF is held across, Human Resources, Quality, Facilities or the IT department, and often what is documented is not always an accurate representation of reality. Given that a cyber-attack comprises of a delivery and an exploit phase and can include a combination of socio and technical elements, in order for an organisation to respond or recover particularly minimising customer interruptions and customer minutes lost, a holistic understanding of PPITF and the interdependencies between them should be considered.

CYBER SECURITY

The UK government define cyber security as the protection of internet connected systems, the data on them and the services they provide. This includes harm caused intentionally or accidentally. [1]

A cyber-attack can originate from:

- foreign intelligence services or
- industrial competitors, looking to destabilise an organisation or country to obtain an economic advantage,
- hacktivists, who have a political or ideological motivation,
- hackers or script kiddies, who like the challenge of interfering with an organisations computer systems, or
- employees, who might cause unintended or intentional damage, considered the biggest threat in cyber defence, but also the greatest strength for recovery.

A cyber-attack typically comprises of two phases, a delivery and an exploit phase. The delivery phase, is positioning the attack so that it can be exploited; the exploit phase will have an overt or covert effect on the organisation.

It was predicted that the spending on information security products and services would grow to $93 billion in 2018, this was mainly predicated on the rising awareness from CEOs and boards of directors about the business impact of security incidents and an evolving regulatory landscape

[2].

Deploying technology is an obvious step but provides limited mitigation against a cyber-attack. It is naïve for an organisation to think that implementing cyber technology will keep it completely secure, and help it recover, from a persistent attacker.

Typically an organisation should use some sort of framework to enable it to understand and manage its cyber security risks. There are a number of different frameworks which are available to be used, however one of the more ubiquitous frameworks is NIST (National Institute of Standards and Technology). In the US, the Presidential Office has signed an executive order to mandate that all government offices should implement NIST. It comprises of a set of desired cybersecurity functions for managing cyber security risks:

- Identify – Understand organisational construct at risk from a cyber-attack.
- Protect – Limit or contain the impact of a potential cyber-attack.
- Detect – Activities to identify a cyber-attack.
- Respond – Action against a detected cyber-attack.
- Recover – Restore capabilities or services affected by a cyber-attack.

Each function can be further broken down into a number of controls which get to the core of where cyber security risks may persist. As an example for the identify function

1. Are suitably qualified and experienced personnel assigned?
2. Is an inventory of information, systems and technology up to date?
3. Are the legal and regulatory requirements for information security controls identified and documented?
4. Is a coherent and consistent process used for identifying and prioritising information security risks?
5. Are controls in place to ensure the supply chain have an appropriate level of cyber maturity, and that information flows are appropriate?

As is hopefully obvious these controls are not just aimed at technology. There are similar controls for the other NIST functions.

Technology has its place as part of the strategy for cyber defence. It is an integral foundation across a number of the above cybersecurity functions, but it is not the complete solution. This is potentially truer for electricity distribution which is already complex, with a large supply chain and will only get worse with the sector being digitalised.

ELECTRICITY DISTRIBUTION

Within the UK the provision of electricity to consumers spans four different types of organisations:

- Generation plants
- Transmission networks
- Distribution operators
- Supplying companies

Distribution Network Operators take electricity from the transmission networks to the end users, including homes, small or large industry, car charging points etc. Networks comprise of a complex infrastructure of pylons, cables and substations. The distribution of power is however going through a revolution with the generation of electricity becoming distributed i.e. the provision of wind and solar farms, with DNOs provisioning these sources of electricity. The distribution is also becoming smart with the electricity network intelligently integrating the actions of all users connected to it, including generators and consumers.

The effect of a coherent and consistent cyber-attack is not fully understood, and until such time as an attack happens, is its impact being taken seriously by DNOs. Although a dramatization, the 2013 film by National Geographic, American Blackout, gives a graphic and credible representation of the long lasting and profound effect a cyber-attack can have on power distribution within the US.

Scottish Power Energy Networks, are one of the top 6 power companies within the UK. They have about 10,000 employees. They are the DNO for central and southern Scotland, Merseyside, North Wales and parts of Cheshire and Shropshire, as such it has a complex network of facilities. Within the UK the DNOs are ~~heavily~~ regulated by the Office of Gas and Electricity Markets (OFGEM), specifically by the ECSG (Electricity Connections Steering Group), and standards such as the ESQCR (Electricity Safety, Quality and Continuity Regulations), Electricity Act, D (Distribution) Code and G (Grid) Code. With the deployment of the Smart Grid, a vast amount of information is being created.

A HOLISTIC APPROACH TO CYBER SECURITY

As previously stated to effectively protect the electricity network from a cyber-attack, it is not enough to just employ technology. Operators and organisations need to adopt a comprehensive approach considering human, social, cultural, governance and location factors. To support the detection, prevention and correction of cyber security vulnerabilities.

There is an insurmountable management overhead in deploying more cyber protection tools, and tailoring them to be most effective within an organisations infrastructure.

It is also well understood that most attacks target a person for delivery of an attack prior to it being exploited. People can be a vulnerability due to sub-optimal processes or procedures, due to lack of awareness or training or just because they are being malicious.

Psychology and social engineering techniques are both being used to bypass any technology defences and to potentially use insiders as an attack vector. An obvious method by which insiders can be subverted or radicalised is through the use of social media. The use of technology to try and identify, or subvert, the people vulnerability within an enterprise will fail.

When considering the cyber threat to an organisation, there are many different ways of characterising it, one approach which we have utilised is to break an organisation down into PPITF.

- **People**, includes the recruitment, onboarding, training, management and their exit from the organisation.
- **Processes**, includes the policies, procedures and processes, detailing who is responsible for who, what, when and how.
- **Information**, this looks at ensuring that all information, digital and paper is held appropriately.
- **Technology**, this includes not just traditional Information Technology but also the network and cover the procurement set-up and disposal.
- **Facilities**, are the physical locations where work is delivered, for homeworkers this will include individual homes.

There are obvious interdependencies across the different elements of PPITF, and supporting all of them will be some sort of supply chain. This supply chain will have its own cyber vulnerabilities, whether it be recruitment agencies, air conditioning companies, or cleaners.

AN ENTERPRISE VIEW OF AN ORGANISATIONS INTERDEPENDENCIES

Given that for an effective defence to cyber-attacks we have specified the need to consider an organisation in its totality including PPITF. For a system such as a DNO or DSO the elements of PPITF singularly can be quite complicated. When you consider the interactions and dependencies between PPITF, and that an organisation is highly dependent on a number of interdependent systems or capabilities, DNOs or DSOs become highly complex.

For a DNO or DSO it would be completely impossible for a single person to keep a complete understanding of the totality of PPITF and all interdependencies in their head. We would also challenge if what is documented, for an organisation, is a true and up to date representation of the company.

Given the above it makes it very hard to be able to plan or run scenarios, to understand the impact or how to recover from a cyber-attack, either before or after an attack. However by creating a model of your DNO or DSO you are able to undertake some “what-if” analysis. This is where Enterprise Architecture (EA) comes in.

EA utilises graphical models as a vehicle to undertake system analysis, system design and to demonstrate the communication paths between various components or entities. EA adopts architectural models of systems and the organisational environment which underpins the systems. EA provides a set of models to predict behaviour and the effects that changes to discrete systems might have, i.e. the effect from a cyber-attack. However for an EA to be effective a true understanding of PPITF across an organisation is required, not what is documented, or intended but the actual construct.

For an organisation definitive knowledge of PPITF is typically held across a number of people and departments:

- People should be understood by Human Resources departments and by line managers;
- Processes by quality or standards departments, or by the individual departments who they are most relevant for.
- Information, by the IT department, or by the department capturing the information, i.e. for Personnel information the HR department.
- Technology, by the IT department and maybe also the procurement department
- Facilities, by the facilities department often supplemented by knowledge of the admin team.

Our experience is that the information for PPITF is best captured through a series of stakeholder workshops, by using a common taxonomy and consistent set of artefacts, PPITF and any interdependencies can be captured within an EA

By augmenting the organisations understanding of PPITF with potential cyber security vulnerabilities structured around a framework, such as NIST described above. An organisation is able to focus their resources, whether it is money or by deploying their people onto areas of potential high risk or where significant damage might be caused to an organisation.

CONCLUSION

In the past organisations have been seduced into protecting their organisation from a cyber-attack by deploying technology. From a financial or resource perspective this approach is becoming untenable and is not completely effective. Organisations need to adopt a comprehensive approach considering human, social, cultural, governance factors and the broader enterprise, for the detection, prevention or correction of cybersecurity vulnerabilities; sole reliance on technology will ultimately fail.

A holistic approach to cyber need to be considered covering PPITF, this makes the problem very complex. By capturing the actuality of an enterprise within an EA the complex becomes manageable and allows an effective cyber defence of recovery plan to be developed and implemented.

REFERENCES

[1] UK Government, National Cyber Security Strategy 2016-2021

[2] “Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017”