Renewables Consulting Group

CYLANCE™

Public

Cybersecurity in Renewable Energy Infrastructure

Classification	Public
Date	2018-02-13
Revision	V1-0

Sam Park
Director, RCG

+44 7500 896 757
sam.park@thinkrcg.com

Dr. Anton Grashion
Senior Director, Cylance

+44 7919 057 229
agrashion@cylance.com

James Taylor
Associate, RCG

+44 7469 711 220
james.taylor@thinkrcg.com

CONTENTS

© 2018 The Renewables Consulting Group

1 INTRODUCTION

This paper brings together the renewable energy expertise of RCG and the IT system security and protection experience of Cylance, to provide insight into cybersecurity for the renewable energy industry, focusing on threat and impact assessment, and on measures to improve cyber protection.

Recent cyber-attacks such as the so-called 'WannaCry' worm, in which the IT systems of a number of high profile organisations were infected and held to ransom, have led to increasing concern regarding cybersecurity. With the world shifting rapidly towards expanded connectivity, concern is justified, as the spectre of cybersecurity threat is at an all-time high. Attacks are increasing in both frequency and severity; they are becoming harder to prevent due to the ever-evolving nature of the malicious software (malware) employed by attackers. Cyber-attacks are an escalating threat, and have the potential to inflict large financial losses, damage assets, and create national security risks.

The potential impact of cyber-attacks is particularly noteworthy in the energy industry, as conventional electrical energy infrastructure moves towards more distributed but integrated and 'smart' electrical grid systems. Key areas at risk of cyber threats include energy production monitoring, control of production and consumption and the increasing volume of large financial investments associated with generation assets and infrastructure, as well as the increasing global reliance on the energy it generates. The significance of the threat not only lies in its severity, but in its unpredictability and reach. Malicious actors in one corner of the globe have the capability to launch attacks on vulnerable energy assets in a different country or continent, making it increasingly difficult to predict when, where and how a cyber-attack will happen.

Renewable energy generation assets comprise a key and fast-growing portion of the energy industry. As the world switches to a clean energy future, the dependence on renewable energy is likely to increase further, meaning the cybersecurity of such assets is of paramount importance.

2 CYBERSECURITY AND KNOWN THREATS

Renewable energy technologies have established a significant role in the energy industry, with over 2000 GW of global electrical energy capacity installed as of 2016[1]. As nations strive to meet the clean energy targets set at the Paris Agreement[2], this figure is expected to grow for the foreseeable future. Because of their prominence and the world's increasing reliance on the energy they generate, it is vital for the industry to develop security, and specifically cybersecurity, strategies driven by wider knowledge and experience.

2.1 Considerations for Protecting Critical Infrastructure

Cyber-attacks targeting critical infrastructure have increased over the last ten years according to a recent survey of twenty nations[3]. While Critical Infrastructure Protection (CIP) is essentially a government responsibility, in several western nations critical infrastructure is privately owned. This dual ownership creates complexity resulting in inefficient and redundant security coverage. To further complicate matters, Critical Information Infrastructure Protection (CIIP) is essentially a global problem due to the worldwide nature of information networks (telecommunications, internet, IT, etc.) leveraged by critical infrastructure. The very nature of CIIP demands that governments and private enterprise collaborate to foster strong protections for critical infrastructure.

Cybercriminal groups like 'Energetic Bear' and 'Gothic Panda' are of particular concern to the renewable energy sector. In 2013, Energetic Bear targeted the western energy sector with 'watering hole attacks' (the use of infected websites of interest to employees) to gain access to critical infrastructure[4]. In 2014 Gothic Panda unleashed a 'spear phishing' campaign against western energy

[1] *Renewable Capacity Statistics 2017*, (IRENA, 2017)

[2] *Climate Get the Big Picture,* (UNFCCC website accessed 2017)

[3] P*rotecting Critical Infrastructure from Cyberattack*, (Cabrera, 2016)

[4] *Energetic (Russian) Bear Attacking Western Energy Sector*, (info-security Magazine 2014)

companies[5]. This same year another group named 'Black Energy' developed malware which infected Ukrainian power networks.

Typically, uncoordinated security practices ensure that western critical energy infrastructure remains a prime target for cybercriminals for the foreseeable future.

2.2 Current Trends in Cybersecurity

In the US, Forbes Magazine predicts economic losses due to cyber-crime will reach US$2 trillion within the next two years. They note that the costs incurred by cybercrime quadrupled from 2013 to 2015 and believe this trend will repeat by 2019[6]. Foreseeable threats include continued growth of the 'Dark Web' (where illegal information and products are traded), Distributed Denial of Service (DDoS) attacks, state-sponsored cyberattacks, and widespread spear phishing attacks.

While a comprehensive list of all cybersecurity threats is beyond the scope of this document, there are numerous threats of particular importance to renewable energy companies:

2.2.1 Ransomware

Ransomware attacks typically encrypt a host system and hold data hostage unless the victim pays for decryption. Ransomware attacks similar to those which affected the Hollywood Presbyterian Medical Center (Locky) and global threats like 'GoldenEye', 'CryptoLocker', and WannaCry continue to thrive. ZDNet reports the ransomware market on the Dark Web increased twenty-five-fold from $250,000 in 2016 to $6.24m in 2017[7].

A survey of IT managers conducted by the Enterprise Strategy Group (ESG) revealed that 81% are concerned about ransomware[8]. Another 16% of respondents are monitoring this type of malware closely.

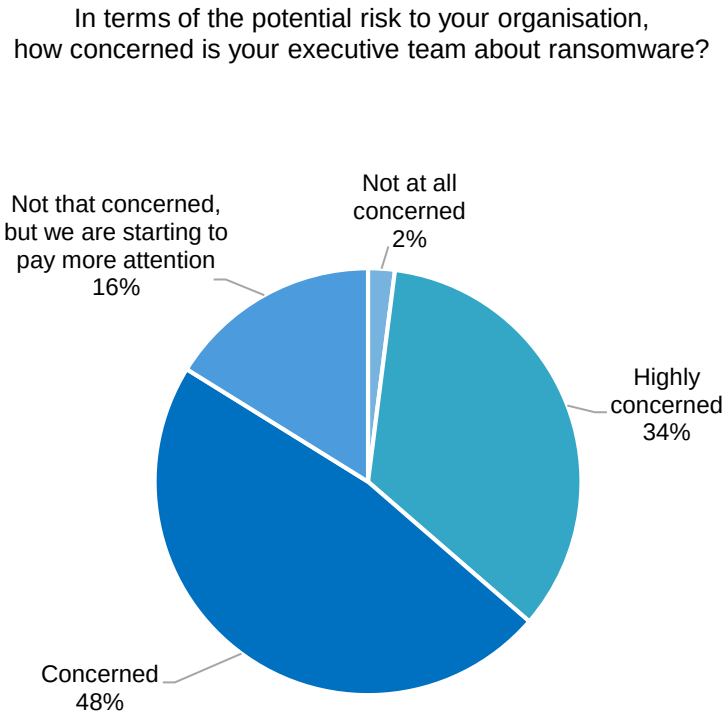
[5] *China-Linked APT3 Group Focuses Attacks on Hong Kong*, (ICIT, 2016)

[6] *Cyber Crime Costs Projected To Reach $2 Trillion by 2019,* (Forbes, 2017)

[7] *Ransomware is Now Big Business on the Dark Web and Malware Developers Are Cashing In*, (ZDNet, 2017)

[8] *2018 IT Spending Intentions Survey*, (ESG, 2017)

Exhibit 1: Executive team concern about ransomware



Source: Enterprise Strategy Group

2.2.2 Fileless Attacks

Fileless attacks, also called zero-footprint and non-malware attacks, utilise legitimate system resources to exploit infrastructure. These attacks rely on tricking users into visiting an infected website where security flaws are leveraged into system access. PowerShell (a programming language and framework), web browsers, or other applications are then loaded into system RAM and used to perform tasks ranging from information hijacking to bitcoin mining. These attacks are extremely difficult to detect as they place no files on the target machine. Fileless attacks has seen double-digit growth since the beginning of 2016[9].

[9] *What is a fileless attack? How hackers invade systems without installing software*, (Korolov 2017)

2.2.3 APTs and Trojans

Advanced Persistent Threats (APTs) generally target specific organisations and follow a systematic workflow (or 'kill-chain') process to gain access to IT infrastructure. An APT attack includes the following features:

- Advanced – Cybercriminals use a wide variety of intrusion technologies. These technologies or techniques are modified as necessary to remain effective in response to detections or countermeasures.
- Persistent – The attack is launched with a specific objective or objectives and is actively monitored. Targets of opportunity are ignored. The attacks continue until objectives are met.
- Threat – The attack is coordinated to some degree by skilled human operators. These operators are generally organised and well financed.

Trojans are programs that enable unauthorised third-party access to IT systems. They may be disguised as legitimate programs to trick their targets into willingly installing or executing them. Once a system is compromised, backdoor access is enabled to allow attackers to infiltrate and execute commands. Unlike viruses or worms, trojans do not try to replicate themselves or inject themselves into other software.

2.3 Cybersecurity in Renewable Energy

A renewable energy asset's security can be broken down into two main components that are directly linked; physical security and cybersecurity. A successful cyber-attack has the potential to damage a project's physical assets through the forced maloperation of components, impact its finances by disrupting generation, or create national, or regional, energy security risks in the event of a large-scale grid blackouts.

Although historically they have not been a common target for cyber-attacks, large scale renewable energy assets can have vulnerabilities that attackers could exploit – namely their distributed and remote nature which tends to create more challenging physical security issues.

The threats to renewable energy generation assets should be viewed in the context of wider threats to the energy industry, and examples are provided in the succeeding subsections describing recent attacks on the energy industry and known threats to renewable energy generation assets.

2.4 Examples of Attacks on Energy Companies

Two examples are provided here of known attacks on energy companies; an attack on Aramco in 2012 and a series of attacks on the Ukrainian electrical grid

system between 2014 and 2016. Both of these examples are pertinent to the renewable energy industry.

2.4.1 Aramco

Saudi Aramco suffered a devastating cyber-attack in August 2012. An employee had visited an infected weblink which allowed a wiper virus (deletes data) to install and propagate across the Aramco IT infrastructure. Within hours, 35,000 company computers were completely, or partially, destroyed, gasoline refill stations went offline, and corporate email and phone systems were terminated[10].

Aramco responded by directing their offices to disconnect all devices from the internet. Over the next five months Aramco conducted its business via the use of typewriters and fax machines. They endured massive expenses by donating oil to domestic consumers (to stem an energy crisis) and bulk-purchasing 50,000 computer hard drives at above-market prices. A group named 'Cutting Sword of Justice' claimed responsibility. To date, no one has been arrested and prosecuted for the attack.

2.4.2 Black Energy

APT and trojan attacks, authored by the so-called Black Energy group, raged through the energy sector beginning in 2014. The attacks were widespread but particularly devastating to Ukraine where power grids were taken offline in December 2015 and again in December 2016. The 2015 attack left a quarter-million Ukrainians without power for six hours as over fifty power stations were shut down. In 2016, another attack brought down an electrical substation which supplied more power than all the targets of the 2015 attacks combined. Russian secret security forces are widely suspected of staging these Black Energy attacks[11].

Black Energy attacks use a wide array of techniques including spear phishing, trojans, DDoS, and information destruction. The attackers adapted to countermeasures by changing their injection methods from infected Microsoft Excel macros to infected Microsoft Word documents. In 2015 several power stations were taken offline via the remote commands of cloned control software. In 2016 the attackers changed tactics and seized direct control of the electrical substation control room computers to force a shutdown.

Attacks undertaken at the electrical grid system level would also impact all connected renewable energy generation assets. Black Energy malware has been found in the critical infrastructure of other nations including Poland and the

[10] *The inside story of the biggest hack in history*, (Pagliery, 2015)
[11] *How an Entire Nation Became Russia's Test Lab for Cyberwar,* (Greenberg, 2017)

United States. Cyber-attacks targeting renewable energy assets and power systems are therefore a significant and genuine threat.

2.5 Known Threats to Renewable Energy Generation Assets

Two examples are given below of known threats to onshore wind and solar assets respectively. Whilst no specific threats to offshore wind assets are discussed, the threats are similar in nature to those of onshore wind. However, assets far offshore would introduce additional, though not insurmountable, physical access challenges to would-be attackers should such access be necessary for the purposes of the attack.

2.5.1 Mock cyber-attack on a US onshore wind farm

Recently, researchers from the University of Tulsa, Oklahoma, carried out a mock cyber-attack on a US onshore wind farm with the permission of the associated wind energy company. The purpose of the mock attack was to demonstrate the potential threat of cyber-attacks[12]. The researchers successfully bypassed physical security by picking the lock of a single wind turbine and connected a Raspberry Pi minicomputer to the ICS network switch (a component of the turbine operation control system). The researchers then gained access to the control systems of all turbines in the wind farm, enabling them to repeatedly start and stop the machines. Repetitive loading of this nature could, over time, lead to the premature degradation of gearbox, clutch and brake systems, all of which would be detrimental to operating costs and potentially to the lifetime of a wind turbine. In the worst-case scenario an attack of this nature could lead to catastrophic failure and subsequent total loss of a turbine. In addition, the researchers proved they had the capability to install a piece of software that could fabricate or replay false signals and transmit them to the turbine operators; theoretically an attack could therefore take place without detection.

2.5.2 Known Threats to Solar Photo-Voltaic Assets

Vulnerabilities at solar photovoltaic (PV) plants have also been investigated[13]; a Dutch security engineer has theorised and published the possibility for a large scale cyber-attack on solar PV installations which could lead to widespread power outages. An analysis and field test on the vulnerabilities of DC/AC inverters employed at solar PV farms revealed that this situation is technically

[12] *Wind farm security: attack surface, targets, scenarios and mitigation*, (Staggs et al., 2017)

[13] *Horus Scenario, Exploiting a weak spot in the power grid*, (horusscenario.com, 2017)

feasible. The study reveals that although a scenario of this magnitude would be difficult to achieve; the social and financial implications of a large-scale grid blackout are severe.

3 THE CYBERSECURITY RISK

Maintaining a secure computing environment is a top concern for IT managers across the globe. This is reflected by a recent ESG survey which asked how technology managers justify their funding[14]. Renewable energy companies would likewise benefit by investing in information security. Achieving a secure environment includes dedicating resources to physical security, hardware and software, internet connectivity, remote management, and training personnel.

Exhibit 2: IT investment justification

Source: Enterprise Strategy Group

[14] *2018 IT Spending Intentions Survey*, (ESG, 2017)

3.1 Physical Security

In the absence of an internet connection, when defending against cyber-attacks, a renewable energy asset's first line of defence is its physical security. Renewable generation assets are often situated in remote locations as developers seek the most suitable energy production conditions for their technologies, and hence the physical protection of installations is difficult to both monitor and respond to in the event of a security breach. A physical security breach not only opens the possibility for equipment sabotage, but also introduces cybersecurity vulnerability. In this situation, to initiate an attack, cyber-attackers would need physical access to supervisory control and data acquisition (SCADA) systems, individual machines (turbines in the case of a wind farm) or ancillary control systems. The researchers from the University of Tulsa demonstrated the severity of this threat, should the physical security (fences, CCTV, alarms, locking devices) of renewable assets be neglected.

3.2 Inadequate and Outdated Hardware and Software

Characteristically, malware continues to develop and evolve over time. Therefore, typical off-the-shelf preventative software must be frequently updated to ensure it can detect the most recent properties or behaviours of malicious programs; if not kept up to date, certain security software can be useless in the defence against malware.

Over the typical 20-year lifespan of a renewable energy asset IT technology will progress significantly. Therefore, installed IT technology may not be old with respect to the age of the renewable energy asset, but are likely to become superseded by systems with greater capabilities and features. Hence, more outdated technology may not be able to support modern malware detection methods or will be limited by the capabilities of the installed operating system. Researchers from the University of Tulsa discovered that a number of wind turbine controllers were sending unencrypted messages within their networks and were, at times, using default passwords; all actions known to increase cybersecurity risk. These issues are accentuated by the fact wind turbines are frequently 'daisy-chained' on the same network, with the result that often only a single machine would need to be hacked to gain control of an entire wind farm[15].

[15] *Wind farms and factory robots at risk from hackers, experts say*, (Kuchler, 2017)

Other hardware and software issues are known to be present at renewable energy assets; for example, operators have used public Internet Protocol (IP) addresses for their routers thus leaving their operations and maintenance (O&M) and monitoring software open to attacks[16].

However, actions are being taken to help improve the cybersecurity of renewable assets. For example, in the US before being permitted to access the grid, turbines must meet the Critical Infrastructure Protection Standards which are issued by the Federal Energy Regulatory Commission[17]. The standards cover issues such as sabotage reporting, security controls, and recovery plans.

Similarly, in the UK there are measures in place, such as the government's Cyber Essentials scheme, which is a certification designed to provide organisations with a basic level of protection from the most prevalent threats coming from the internet[18]. However, this scheme is currently only mandatory for those with central government contracts.

3.3 Internet Connectivity and Remote Management

Distributed renewable energy assets are invariably connected to the internet as this gives operators control access to real time data and automatic system warnings. It also enables remote management; multiple wind and solar farms are now controlled from great distances away from the sites themselves. This allows for increased efficiency as personnel do not have to be deployed permanently on site, and the optimisation of generation, as project parameters can be adjusted to maximise energy yield.

However, internet connectivity and remote management also provide an opportunity for cyber-attackers; remote hacking via internet connections allows attackers to remain anonymous and bypass any physical security of a renewable asset, increasing the likelihood of global attacks[19].

A successful cyber-attack on a renewable project's remote monitoring system could create a number of issues, including the ability for attackers to restrict revenue-creating generation or to collect market sensitive data. The remote management risk for renewable energy assets that convert kinetic energy into electricity, such as wind turbines, is inherently greater over more static power generation methods, such as solar PV, as attackers could cause physical damage through repetitive operational commands on moving components at undesirable times.

[16] *Time for solar to step up to cyber threat*, (Parnell, 2017)

[17] *Time for solar to step up to cyber threat*, (Parnell, 2017)

[18] *Procurement Policy Note 09/14: Cyber Essentials scheme certification*, (Gov.uk, 2016)

[19] *Some Wind Turbines Can Be Hacked by Anyone with an Internet Connection*, (Franceschi-Bicchieral, 2015)

3.4 Personnel

Cyber-attacks are not limited to hacking from external parties and can easily occur internally when untrained personnel are allowed access, or if the correct measures are not taken when an employee leaves a company. The training of personnel should occur immediately upon the recruitment of new employees to help ensure they do not inadvertently pose a threat to the cybersecurity of a project. In addition, usernames and passwords of control and monitoring systems should be changed and access levels reviewed periodically and reassigned when any employee leaves a company.

Sufficient personnel cybersecurity awareness training is critical; email phishing was a key technique used by hackers in the 2015 Ukrainian power grid cyber-attack. Attackers sent emails to employees at Ukrainian power utilities that installed malware when attachments were opened. If personnel are adequately trained in cyber-attack prevention, then the risk of attacks of this nature can be reduced.

4 CYBERSECURITY RECOMMENDATIONS

4.1 Assess Your Environment

Renewable energy companies should carry out comprehensive assessments of their current cybersecurity posture before any investment in third-party or in-house security solutions. Several options exist for both self-assessment and outside evaluation.

The US National Institute of Standards and Technology (NIST) provides a free guide for assessing and implementing a cybersecurity framework for manufacturers[20].

The European Union Agency for Network and Information Security (ENISA) is working to standardise security practices across the European Union (EU). They offer compliance guides on their website, including the Governance Framework for European Standardisation and the Definition of Cybersecurity - Gaps and Overlaps in Standardisation.

The EU also offers free copies of its Directive on Security of Network and Information Systems, available in multiple languages[21].

Other security assessment options include third-party vendors, the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, and hiring IT professionals with CISSP, CISM, CISA, ISO/IEC 27001:2013 (Auditor/Lead Auditor), CRISC, or QSA/ISA certifications.

4.2 Keep Assets Up to Date

Keeping both the human assets trained and the IT infrastructure updated is critical. Updated systems provide a last line of defence when other security

[20] US National Institute of Standards and Technology (NIST), https://doi.org/10.6028/NIST.IR.8183

[21] EU Directive on Security of Network and Information Systems, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

measures fail. After a software patch is released, cybercriminals may be ready to exploit unpatched systems in less than 24 hours[22].

The following best practices can assist with keeping systems updated:

- Educate employees on the dangers of out of date systems and software.
- Limit the number of systems using frequently exploited software like JAVA, Flash, and browser plug-ins.
- Use patch management and IT update software or services for mass update roll-outs.
- Enable automatic patching of IT assets where possible.
- Separate networks servicing Bring Your Own Device (BYOD) capabilities from critical system networks.
- Continuously monitor infrastructure for systems that are out of date.

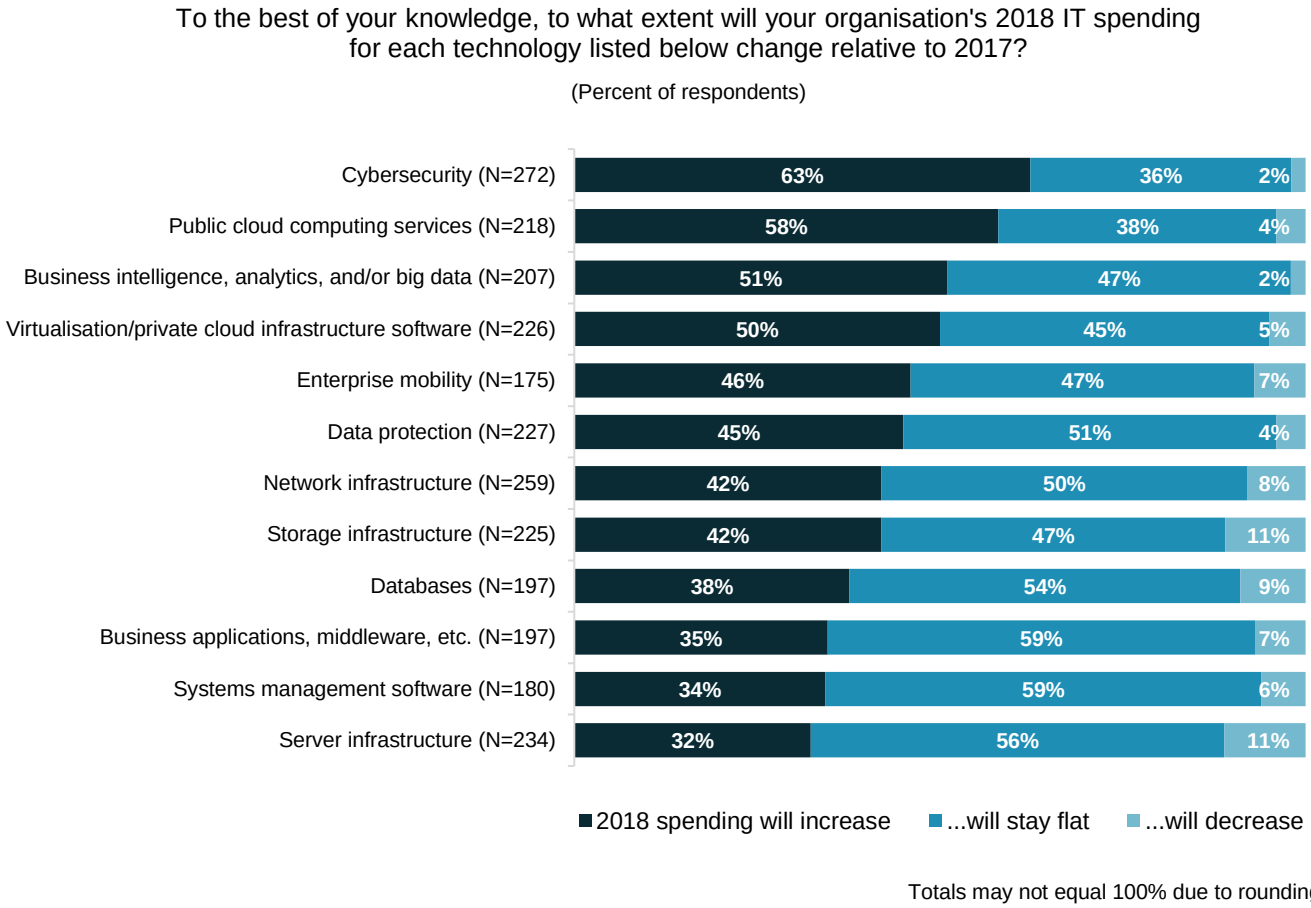
To mitigate risks, patch a test system loaded with your organisation's critical applications and verify that nothing breaks during or after the update process before pushing the patch to the production environment. Utilise rollback strategies to protect against post-update issues that only surface hours or days after the patch. Perform updates simultaneously across the environment to maintain system integrity.

Keeping cybersecurity assets current will be a priority for IT managers in 2018, according to a recent ESG survey[23]. The unprecedent growth of cyberattacks over the last four years makes such expenditures understandable.

[22] *15+ Experts Explain Why Software Patching is Key for Your Online Security*, (Zaharia, 2016)

[23] *2018 IT Spending Intentions Survey*, (ESG, 2017)

Exhibit 3: IT spending change by technology (2018 compared to 2017)



Source: Enterprise Strategy Group

4.3 Access to Sensitive Systems and Data

A recent NIST survey of the energy sector reveals that identity and access management (IdAM) responsibilities are often decentralised and disorganised within energy companies. This creates difficulty in maintaining access control over internal systems and exposes companies to increased security risks[24].

Effective access control requires administrators to have a centralised overview of all current access policies. Admins require the ability to rapidly grant or restrict access in response to a dynamic environment. Individuals should be granted sufficient access to perform their work, nothing more.

[24] *Identity and Access Management for Electric Utilities,* (NIST, 2015)

Access control policy can be based on numerous models including Attribute-based Access Control (ABAC), Discretionary Access Control (DAC), Identity-Based Access Control (IBAC), Organisation-Based Access control (OrBAC), or Role-Based Access Control (RBAC) among others.

4.4 The Predictive Advantage

The rise and increased adoption of artificial intelligence (AI) and machine learning (ML) tools is revolutionising several industries. Everything from product recommendations on Amazon to search results on Google leverage some form of AI/ML to analyse input and predict desired output. By “learning to read” big data, computers can create useful algorithms based upon billions of test cases.

Within the security sector innovative companies have harnessed the predictive power of AI/ML to combat both current and future cyberthreats. By training security AI to recognise and respond to countless file samples they have achieved impressive results. For example, the 2015 version of CylancePROTECT (a company leveraging AI/ML in their endpoint security solutions) can detect and prevent both GoldenEye[25] (released 2016) and WannaCry ransomware[26] (released 2017) before they can execute. This indicates that automated, intelligent AI/ML security systems will offer the best solutions as cyberattacks and operating environments become more complex. An added advantage is that predictive prevention can create a breathing space during which time patching can be planned and rolled out while maintaining a strong security posture.

[25] *Petya Returns as Goldeneye Strikes Germany,* (Cylance, 2016)
[26] *TITAN SI Tests: WannaCry Ransomware vs. 8 AV solutions,* (Yong, 2017)

Renewables Consulting Group

The Renewables Consulting Group

RCG is a specialized expert services firm dedicated to the global renewable energy sector. We are a firm of practical consultants known for our technical expertise, Industry foresight, and sleeves-rolled-up approach to projects. From strategy to implementation, we serve businesses, governments, and non-profits around the world with technical, commercial, and management consulting services for the public sector, private equity and financial services firms, utilities, independent power producers (IPPs), and contractors and manufacturers for land-based and offshore wind, solar, hydrokinetic and ocean energy, and energy-storage technologies. RCG is headquartered in London in the United Kingdom, and has offices in New York in the United States.

London

Gilmoora House
57 – 61 Mortimer Street
London
W1W 8HS

New York

433 Broadway
6th Floor
New York
NY 10013

For further information, please visit www.thinkrcg.com

Copyright © The Renewables Consulting Group 2018
All rights reserved