National University of Ireland, Cork

School of Engineering
Chair of Information Technology in Architecture, Engineering & Construction

Module: CE6014 Computer Mediated Communication
Assignment: Information Security- Protection and Access of Data
as part of MEngSc
Information Technology in Architecture, Engineering & Construction
Academic Year 2018/2019
November 2018

INFORMATION SECURITY- PROTECTION AND ACCESS OF DATA

By .
Name: Colin Perry
Student ID: 117223826

Lecturer: Ass. Prof. Dr. Matevž Dolenc

Declaration

I hereby declare that this thesis is my own work and effort and that it has not been submitted anywhere for any award. Where other sources of information have been used, they have been acknowledged

Signature: 

Print Name: Colin Perry

Date: 11_NOV_2018

Table of Contents

Table of Figures

Table of Tables

1 Introduction

In this assignment students were assigned the task of producing a report that would convince a company to use the technology, platform or software developed.

This project reviews the possibility of producing code that will detect the external connections to a system whether a Building Management System or a BIM model.

With the collaboration and information sharing required for building management systems or any project using data or a modern BIM project, protecting the data is paramount.

That data needs to be protected from unauthorised changes yet available to only those that should have access. It will also need to be available to those that need it for construction purposes, without the ability to change it. The biggest weakness in any system is generally the people with access.

The idea of people leaving some data in a briefcase is insignificant compared to loss of data through a data theft or corruption particularly of a BIM model.

This project will explore methods of ensuring the right people have access:

1. Whom has access, how to provide sufficient access for those who need it,
2. I will review how home working and modern work methods can impact data security.
3. Change control
4. Changes in roles within the lifecycle of the project.

Taking a review of whom else has access to the data through software agreements and legislation.

With the modern society and our connected world how penetration testing of the network can assist in keeping data secure. A test case was run on a BMS system, with the results being explained in this report

Exploring simple measures which can assist in preventing unauthorised users gaining access to systems. Access with two factor authentication and other secure measures.

2 Authorised Access to Data

2.1 Set Up of the System

The system is important as correct set up will mean fewer issues going forward and a reduced potential of a security breach. I will be drawing on experience from a recent penetration test of a BMS system to highlight the need for some of these items.

Network Perimeter Defences – These need to be established prior to data being loaded and connected to an external environment. They form the initial line of defence for protecting the system from external threats. The solution includes the implementation of Firewalls and Internet Gateways.

Malware Protection – This should include client anti-virus. Client anti-virus and malware is in some ways the last line of defence for your business against a cyber security breach.

Patch Management- this should be for all devices not just windows or client devices, but also all network devices. Flaws in software, network and device design are unintentional errors in design that are exploited by attackers. Ensure that proper patch management is in place so that systems are proactively updated with software and application updates. Updates are brought out to counter the influence of hackers within the system.

In a recent test of a building management system it was found that security patches had not been applied to all the system devices. The pieces of equipment that had been forgotten were the network devices. The application of patches needs to be as quick as possible after release, continuously monitored and rigorously applied to all devices in the network.

BMS workstations and servers use a number of different operating systems. In all cases, an official process needs to be in place to update these hosts, or the software they run, including Anti-Virus. If not, a possible result is the multiple hosts being vulnerable to known security issues with published exploits. This may enable an attacker to gain remote code execution on the hosts from anywhere on the BMS network.

The process for the security updates was not in place which allowed insecure updates to be applied to devices. The tool which allows an engineer to configure the BMS controllers had an operational defect. When the engineer selects to connect to a controller, the application checks that it has the right version of the code required to talk to that controller. In order to do this, the tool first checks that it has the latest version of the Java application by querying the BMS components to get a version number. If the version is newer than the tool, then the tool will download a newer version.

Another instance was where an HP ProCurve network switch had no password set. The switch discovered on the network allowed login through its web interface with a blank password. This could allow an attacker to cause disruption by introducing

adverse configurations to interrupt port functionality and also change the password to delay recovery efforts.

Configuration Security; All networks and devices that use the default standard configuration are often easy prey for hackers. It should be ensured that all default passwords are changed, unnecessary user accounts are removed and unapproved default connections on servers, network devices, desktop PCs and laptops are disabled as a starting point. Limiting data permissions is also a good tactic that will limit the extent of damage meaning that only a subset of data is affected.

Where passwords are required for systems where engineers may need to access so a common password is required. These should be changed periodically and sent to the approved users so that only they can access the data/ system.

Again during a recent penetration test of a BMS system it was found there was an instance of a database in MSSQL in use with publicly disclosed credentials. The MSSQL server runs on the BMS workstation and server as well as the engineer's laptop. This is understood to be necessary so that backups can be performed between these devices. The 'sa' user for the workstation and the laptop was found to use the password 'XMG*****1' that has been banned within the BMS providers organisation since its public disclosure. There was no process to discover, review and amend databases that had this setup, by the BMS company.

Web based access is a vital component for BIM collaboration and BMS systems, so the set-up, management of devices and software is a key safe guard to defeat any attack.

2.2 ACCESS PROTOCOLS

2.2.1 Security Measures

People are the weakest link in any system. They are creatures of habit and we all like to keep with things we know. That is why we write down passwords, use words we remember, repeat passwords and use the same password for multiple systems.

Security starts with physical building security and visitor protocols. Initially this may not seem a key means of protecting data, but cyber security attackers can use social engineering tactics to manipulate staff and get around secure network access. If people can not access the building it makes it harder.

Cyber security and ensuring only the right users have access. This will need to be by creating personal accounts on the BMS or BIM model. If possible, it should be linked to the company network credentials. That way any change in circumstances which restricts access to the company systems, will also restrict access to the online BIM model or BMS. It also means the person will have to be logged on via a company approved method. Most companies require login on a company specified device, with a virtual private network. This means the data is encrypted before the Internet Service Provider or the WiFi provider sees it, keeping it secure.

If this is not possible the following should be applied:

A password change will be required every 90 days,

The password must comply with the security standards which require that you follow these guidelines for creating a password:

♦ Must have at least 12 characters

♦ Cannot be the same as a recently used password (last 12 occurrences)

♦ Cannot contain your first or last name as part of your password

♦ Minimum password age must be at least 2 days.

♦ Must contain characters from all of the following 4 categories

1. English uppercase characters (A through Z)
2. English lowercase characters (a through z)
3. Numerals (0 through 9)
4. Non-alphabetic / numeric characters (i.e. !, $, #, %, etc.)

There will also be a reminder on the system that this is the property of the company and it is restricted for official business only.

2.2.2 A Note on Passwords

There are two schools of thought on Passwords for best protection at this time.

The first is to make it long. Security experts agree that a password should have a minimum of 12-14 characters. Richard Cassidy, technical director of cyber security company Alert Logic, says a 14-character password could take 811 trillion guesses to crack. “Length is the thing that gives you protection, not complexity,” he says, adding that even eight-digit passwords can be cracked in a matter of hours. (Guardian, 2018)

The second is to make it unpredictable and unique. The password “qwertyuiop” is the 22nd most used password as it avoids normal words. People then try passwords like “2BorNot2Be” which are far more likely to be picked than things like “HbZBSz44Q5”.

Having reviewed articles in wired (WIRED) the Guardian (Guardian, 2018), and Bomgar. Com (Bomgar, 2018) the best method unpredictable character sequences of longer than 14 characters.

2.2.3 Additional Authentication

Two factor authentication system for users should be deployed using a secure ID Key like the one shown below or a version from an electronic source such as Google Authenticator. These will be supplied, monitored and remain the property of the company operating the BIM model or BMS system. That way in addition to the company credentials there is a component which remains with the owner.

Should a person no longer need access to the project the secure key will need to be returned. Any loss or theft of a key will need to be reported. This will apply if a phone is lost or stolen which as an account and authenticator key software for use with the system.

As the system is web based whether cloud or on servers the authentication protocols can be applied. It is also possible to confirm credentials at set durations after two hours. Normally this is done after periods of inactivity. Also, at the end of a user making changes, so that the user is validated and confirmed to make the changes. This need only be entering the Secure ID code or answer a prearranged validation question.

The work place practice is changing with companies allowing more and more people to work from home. As the system will require authenticated access, including login from a company system this should be encrypted from end to end. Any access will need to be via a virtual private network.

All of these requirements would need to be defined in the Master Information Delivery Plan for the BIM system so that all companies involved in the project are aware of the requirements, planning accordingly.

If the model needs to be moved, copied or deleted from a server there needs to be a higher level of password protection. As part of the system security a dual password entry is required for these administrative changes. This is where two people know half the password. These parties will change as roles change through the life cycle of the facility. There will be more on this in the next section.

Undertake User Training & Education. As mentioned previously, user error is one of the key reasons why networks are breached. As a result, user education needs to be top of the list as one of the best defences.

2.3 BIM MODEL PHASES

2.3.1 PAS1192-2 Phases

There are three main phases within the BIM process and depending upon where the facility is in it's life cycle depends which phase it is in. Fig 2. These phases are design, construction and operation after handover. This cycle may be run through many times in the lifetime of the facility as parts of the building are re-purposed, re-modelled or refurbished.

The event diagram in figure 2 is based on Figure 7, p.13 BS 1192-2 (2013), representing the major steps of the Suppliers Information Exchange (SIEP) and the Employers Decision Points (EDP). The complete diagram is shown in figure 1. figures 2 and 3 show this in more detail.

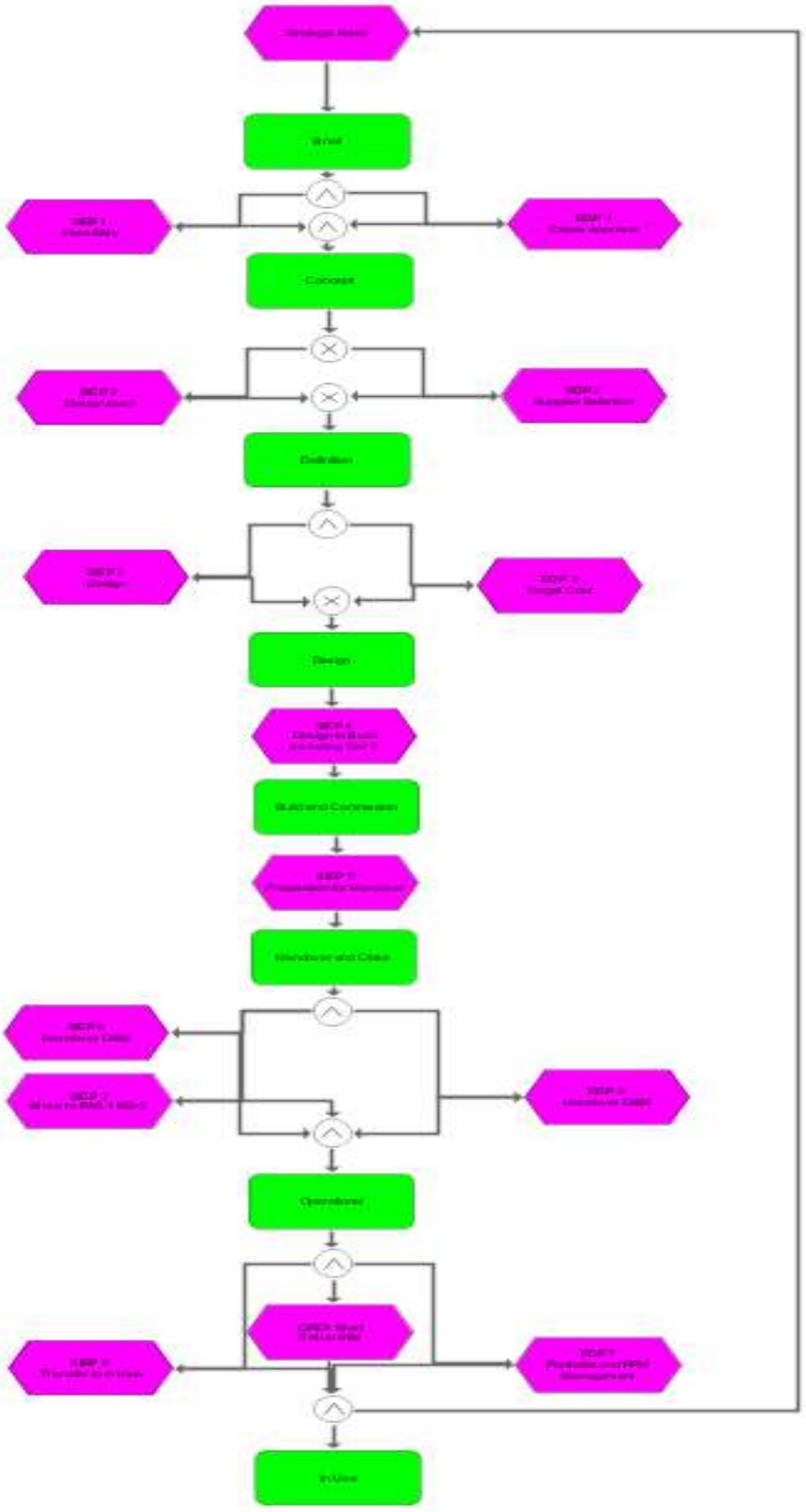

Figure 1: Event Diagram based on Figure 7, p.13 BS 1192-2 (2013) (BSI, 2013)

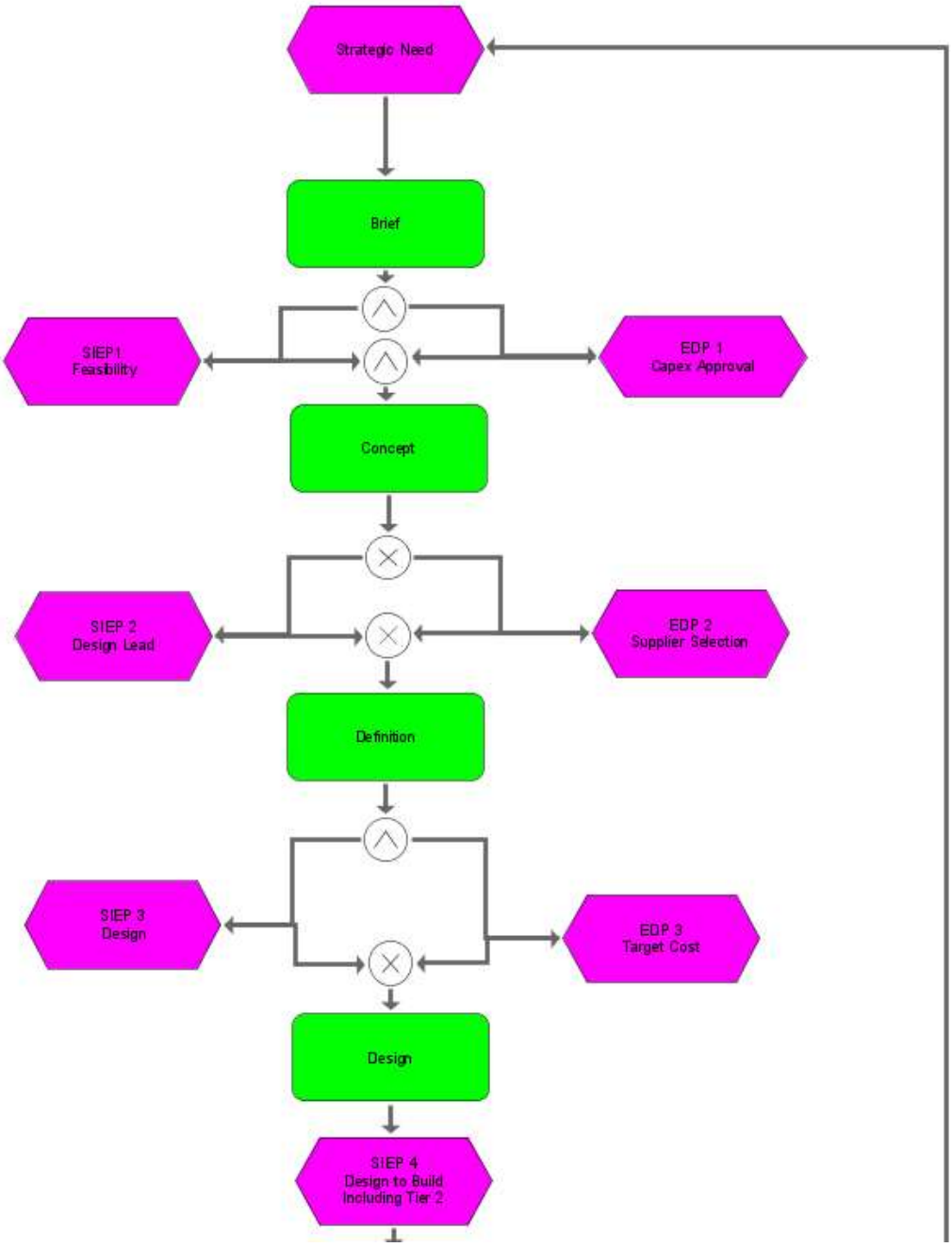

Figure 2: Event Diagram Strategic Need to Design

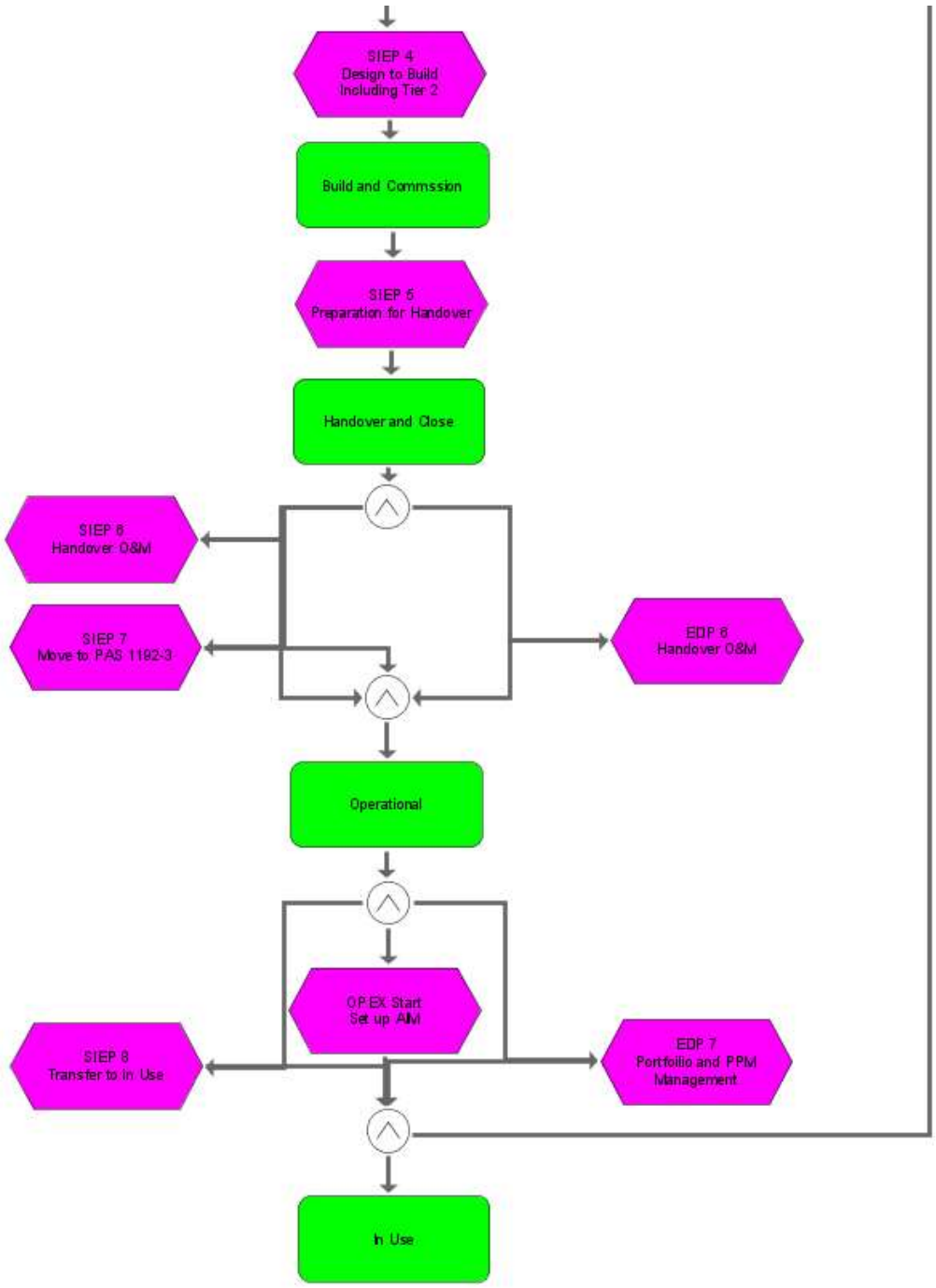

Figure 3: Event Diagram - Build to In Use

The Information Manager has the key role in facilitating the management of the IM model and the production of project outputs. That person is also responsible for managing the operation, standards and culture of the common data environment. The information manager is not a standalone role and is expected to shift from design team to contractor prior to start on site. Under the BIM Protocol, a client is obliged to appoint an information manager at all project stages.

Where in the previous section we discussed having two people with the ability to agree major changes with a joint password. This should be the information manager and the client. This would normally be the client representative on the project or the technical advisor/ resident engineer. The client is the common factor between all of the phases and is responsible for the appointment of the information manager. This would include in the operational phase after handover under Pas 1192-3.

When in the operational phase many organizations may combine the roles of data manager and asset information manager. However the role should include information management as defined in PAS 1192-2.

2.4 Location of and Legislative Access to Data

The aim of all organisations is to ensure they know whom has access to their data and whom has accessed the data, whether directly authorised by the organisation or not.

There a few main items to be considered when setting up the cyber security around a project or network

To ensure all authorised users and only authorised users are able to access the data

We finally come to where the information should be located. This could be on individual servers within the office, remotely located in an owned data centre, a non-owned co location space or on the cloud.

We will deal with what the organisation cannot influence. The legal request from a government body cannot be controlled by an organisation nor in many cases will the organisation be notified. Most datacentre providers, and cloud computing companies have two clauses in their contracts which confirm they are going to comply with legal requests made by governments and courts in many countries. In the case of cloud computing companies, they also have clauses regarding data transfers.

If we look at the Google privacy policy on page 24 it confirms they will comply with every request after a legal review and they will push back in certain conditions. This is common in other company's policy statements. As seen in figure 4.

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

Figure 4: Google Privacy Policy Extract Page 24 (Google, 2018)

For computing companies where information is held on their servers there are also clauses enabling them to transfer data to servers in other countries where their laws will apply, Googles privacy policy also covers this and an extract is in figure 5.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

Figure 5: Google Privacy Policy - Data Transfers Page 14 (Google, 2018)

The US Government has the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) enacted in 2018 after the case US v. Microsoft, a case that was heard before the Supreme Court on February 28th 2018. Where for three years Microsoft had challenged that data held on foreign servers had to have a court order from that country to be released. The CLOUD Act was introduced following difficulties that the Federal Bureau of Investigations (FBI) had with obtaining remote data through service providers through SCA warrants, as the SCA was written before cloud computing was a viable technology. There requests have increased by 70% since 2009.

The US government If the government wins in the Supreme Court, the Sledkom (Russian Law Enforcement) will have a much stronger argument to force Microsoft (or others) to comply with similar requests “We are only asking you to do for us what you already do for the American government.” and if they do not comply hold Microsoft or any technology company in contempt. That would also enable all governments to follow suit enabling countries such as Somalia, South Sudan, Uganda, Nigeria and Syria to make the same information requests. All of these countries are named in the top 30 most corrupt countries in the world (US/ European view). (Google, 2018)

The principle issue with this is not one of politics or national security but a corrupt official after receiving an inducement (bribe or threat) can obtain the necessary permissions to insist a technology company has to hand over confidential data. Therefore, any data stored on servers owned by the technology company could be sequestered by corrupt officials for espionage purposes. Knowing about the risk enables us to ensure we protect our data.

Others have recognised this and a team of developers from the European Organization for Nuclear Research (CERN) has launched a new encrypted email service that could put an end to government snooping. The system, called works by encrypting the data in the browser before it ever comes into contact with the server. So, even if someone

gains complete access to the server, it won't do them any good because the system does not store the encryption key.

The system ProtonMail was conceived by Andy Yen PhD, after a review with fellow scientists examined the issues with online privacy and they were prompted to develop the service following revelations made by former NSA contractor Edward Snowden.

The data we use daily and in BIM models for the most part will have limited interest to outsiders unless they can delete the data to disrupt our business. With suitable back-ups in place a cloud-based solution can be deployed. The US government's Department of Defence is going to a cloud-based solution for some of its applications project is referred to as JEDI (Joint Enterprise Defence Infrastructure) and the winner of the outsourcing should be known over the next couple of months. (Com, 2018)

This risk is very limited but needs to be shared. In conclusion the clients desire to have the model hosted on the cloud should not be changed by this information. Only their awareness of the risk.

3 Penetration Testing

3.1 INTRODUCTION

With regard to ensuring that only those legitimate connections are connected to a network, we have to have connections to enable access to the data. To do this we need to be able to detect what connections are in place for both internal and external connections.

To see if was possible I conducted a limited test on a BMS system. One direct to the system and no connectivity to the internal company network. This simple text code was able to confirm only one connection as it was supposed to be.

The exact text has been amended with #SITE# to replace the site name and #CLIENT# to replace the client name.

3.2 PENETRATION CODE

```
$writeTime = Get-Date
$filePath = "C:\TEMP\#SITE# 131035 Internet Connectivity Test.log"
$nlm = [Activator]::CreateInstance([Type]::GetTypeFromCLSID([Guid]"{DCB00C01-570F-4A9B-
8D69-199FDBA5723B}"))
$nlm.GetNetworkConnections() | ForEach-Object {
$output =[PSCustomObject]@{
NetworkName = ($_.GetNetwork().GetName());
ComputerName = $env:computername;
isConnectedToInternet = $_.isConnectedToInternet;

}
} | Format-Table -AutoSize

"********----------********----------********----------********----------********----------  "  |
Out-File -Append $filePath
"[ #SITE# 131035/Internet BMS Connectivity Test] " | Out-File -Append $filePath
$writeTime | Out-File -Append $filePath

" " | Out-File -Append $filePath
"[START OF INTERNET CONNECTIVITY TEST] " | Out-File -Append $filePath
" " | Out-File -Append $filePath

$output | Out-File -Append $filePath
" " | Out-File -Append $filePath
"[END OF INTERNET CONNECTIVITY TEST] " | Out-File -Append $filePath
" " | Out-File -Append $filePath
"++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ " | Out-File -Append
$filePath
" " | Out-File -Append $filePath

"[START OF #CLIENT# NETWORK CONNECTIVITY TEST] " | Out-File -Append $filePath
" " | Out-File -Append $filePath
```

```
"Is this PC is connected to the #CLIENT# network? " | Out-File -Append $filePath

test-connection 169.86.43.52 -count 1 –quiet| Out-File -Append $filePath

" " | Out-File -Append $filePath
"++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ " | Out-File -Append
$filePath
" " | Out-File -Append $filePath

"NOTE: Results MUST be FALSE for Client Network test, Internet connectivity should be registered
connection address for audit to be successful"| Out-File -Append $filePath
" " | Out-File -Append $filePath

"If Result is TRUE for client network test, contact #CLIENT# GRE BMS Owner IMMEDIATELLY!!!
" | Out-File -Append $filePath
" " | Out-File -Append $filePath
$writeTime = Get-Date
$writeTime | Out-File -Append $filePath
"[END OF TEST] " | Out-File -Append $filePath

" " | Out-File -Append $filePath
" " | Out-File -Append $filePath
" " | Out-File -Append $filePath
```

Figure 6: BMS Penetration Testing Script

3.3 LIMITATIONS AND SUMMARY

The test is run manually at different times to try and detect any anomalies. This code is sufficient for a limited network but would not be suitable for testing on major networks. It would also not detect an intruder on a network with multiple legitimate access points, particularly where they may have legitimate access to other areas of the network.

It is also limited in terms of detecting the connections. If there is a Bluetooth or wireless connection with nothing connected it will not be detected.

Therefore, a second stage is required to the test whether there are any bluetooth or wireless routers connected. When we tested a facility, a wireless hub was found connected to the BMS but as there was no external connection when the penetration test was run it was not detected.

The penetration test of a cloud-based system is beyond my capabilities at this time. It would also require the hosting company to be fully aligned. Many risks are better served by good encryption, (using secure implementations of AES, RSA, along with OpenPGP or similar) and proper access management.

It should also be considered that with the US department of Defence choosing a cloud provision partner under the project acronym JEDI (Com, 2018). If these providers have passed US defence standard testing, then the need for a penetration test may be limited.

3.4 TEST SCRIPT USER GUIDE

1. Locate the text file. (May be attached to the mail or located on a shared drive)
2. Open the script
3. Amend the script to reference client name site. These changes must be done at all points the script has been changed to #SITE# and #CLIENT#. No # is required in the text.
4. Copy all of the text.

5. Open Windows PowerShell ISE (x86) from the start menu

6. Paste the copy script in the top half of the page.
    a. Press play
    b. Script will run
7. Locate the script findings

    File explorer

    |_ “C” drive

        |_ Temp

            |_ Open the internet connectivity test file.

                |_ Review the report and convey any anomalies.

4 Conclusions

The set-up of the system is a key component to prevent cyber-attacks. The application of patches needs to be quick, continuous and rigorous to all devices in the network.

- In all cases, an official process needed to be in place to update these hosts, or the software they run, including Anti-Virus.
- It should be ensured that all default passwords are changed, unnecessary user accounts are removed and unapproved default connections on servers, network devices, desktop PCs and laptops are disabled as a starting point.
- Limiting data permissions is also a good tactic that will limit the extent of damage meaning that only a subset of data is affected.
- Any administration credentials are changed regularly so that if they do get published there is a program in place to change them.
- Web based access is a vital component for BIM collaboration and BMS systems so the set-up, management of devices and software is a key safe guard to defeat any attack.

Security starts with access to facilities preventing direct network access to ensure an attacker cannot gain direct access to the network.

Passwords should be long as a 14-digit password needing 811 trillion guesses. Add to this making the password unique and unpredictable is the best protection. A two-factor system should also be deployed to ensure if the password is breached there is a further layer of defence. Major administrative changes should require two people to enter the password.

As roles/ responsibilities change within the lifecycle of the building, though the design, construction and operations it will be necessary to maintain proper access control.

This risk of government snooping is very limited but needs to be shared. In conclusion the clients desire to have the model hosted on the cloud should not be changed by this information. Only their awareness of the risk.

The penetration test script developed has limits and a second stage is required to the test whether there are any Bluetooth or wireless routers connected.

The penetration test of a cloud-based system is beyond my capabilities at this time. It would also require the hosting company to be fully aligned. Many risks are better served by good encryption, (using secure implementations of AES, RSA, along with OpenPGP or similar) and proper access management.

It should also be considered that with the US department of Defence choosing a cloud provision partner under the project acronym JEDI (Com, 2018). If these providers

have passed US defence standard testing, then the need for a penetration test may be limited.

5 References

Bomgar. (n.d.). Retrieved from www.bomgar.com/

BSI. (2013). *Pass1192-2.* BSI.

Com, T. C. (2018). *Why the Pentagon's $10Billion JEDI deal has cloud companies going nuts.* Retrieved from TechCrunch: https://techcrunch.com/2018/09/15/why-the-pentagons-10-billion-jedi-deal-has-cloud-companies-going-nuts/

Google. (2018, May). *Privicy Policy.* Retrieved from Google. co.uk.

Guardian, T. (2018). Retrieved from How to Create Perfect Password: https://www.theguardian.com/money/2016/may/21/how-create-perfect-password-hackers-online-accounts-safe

WIRED. (n.d.). Retrieved from WIRED: https://www.wired.co.uk/article/how-secure-is-my-password-good-strong-password-ideas