5-minute briefing : “Remote Access to IT systems”

This document is presented as an introductory educational guide that aims to highlight some of the main issues that someone new to the subject needs to consider. It is not intended to be a comprehensive briefing and is not a substitute for an in-depth investigation into the wider issues.

We have a rush on at the moment in the world of IT services.

Right now, there is an urgent need for many companies to setup Remote-Working for their staff so that they can continue their day-to-day business operations in the face of calls for medical isolation and advice to restrict movement of people around the country.

Some big changes have to be made to the company’s operating procedures to accommodate Remote-Working. New rules have to be quickly drafted & approved by the organisation’s management team. And in this rush, many safe-guards are likely to be missed, overlooked or down-played. If the organisation is inexperienced with IT systems then the management team needs to be aware of the significant & new risks that Remote-Working opens up.

A big part of business-related IT management is putting in place appropriate controls and *barrier-fences* to reduce or eliminate IT operations that could permit data-leakage of confidential data and cause a breach of data-protection legislation such as GDPR.

As IT engineers, it is our job to facilitate the wishes of our customers but it is also to inform & advise them that changes to their IT systems to add Remote-Working is going to open up some new & significant risks.

And as knowledgeable technicians, we have to impress upon the customer that they need to carefully assess & consider these risks before they make their decision about who and how many employees are given the option to work remotely.

The first of the major headline risks of Remote-Working is an increased risk of **Data Leakage.**

The off-the-shelf Remote-Working tools that most customers will adopt will (by default) side-step most of the internal IT controls that normally prevent data loss. Out-of-the-box, they will permit Remote printer-sharing, remote desktop file-sharing, and remote USB connections, and each of these can be used to side-step the normal IT controls in place for data-protection.

When someone works remotely they are stepping outside of the normal day-to-day office environment which itself prevents a lot of risky IT behaviour. In the office, employees are going to be observed doing something unwise like bringing in an external USB drive and connecting it to an office computer or adding another printer to the office network and printing off a lot of company documents.

It doesn’t matter whether the motivation is a benign desire to simply achieve a task more quickly or whether it is malicious with a wish to steal company data. The end result is the same, with a big chance of data-leakage and a signifcant danger of breaching GDPR legislation.

The second major headline is **Data Connectivity.**

Remote-Working stretches internet connectivity in new and strange ways.

The standard business “broadband package” that provides a customer’s office internet connectivity is unlikely to have enough capacity for anything more than a few remote-working sessions to operate at the same time.

It will typically have a far larger capacity for incoming data than for outgoing data, usually by a factor of 5-to-1. In normal circumstances this is fine because on a normal working day most of the data-traffic is entering the office rather than leaving it.

Adding Remote-Working access to an office IT system turns this on it’s head and stresses the weaker outgoing data capacity.

So there needs to be a discussion with the customer to identify how many employees can comfortably use the Remote-Working facility and to work out who are the priority users if the IT system becomes over-stretched.

If we don’t do this, then everyone will suffer a poor experience or find it so frustrating that they fail to make use of the system at all.

The third major headline is **Cyber Security.**

Remote-Working makes wide and open connections through the normal firewall defences of the office network.

At short notice, there may be a desire to let employees Remotly connect to the office from their own personal computers at home. This is not an ideal situation as an employee’s personal computer is not under the management of the company, and may have malware or other malicious content hiding on it.

If the decision is made to use personal computers, then extra care needs to be taken because there is a real chance of delivering Ransomware into the office network and letting company data leak out.

Inevitably, any openings that we make to let authorised employees to gain access can sometimes be exploited by bad-operators. If these Remote-Working access routes are un-monitored or even weakly protected then the risk of a cyber-security break-in is significant.

The final headline is **managing customer expectations.**

The simple phrase of “Remote-Working” covers a huge umbrella of technical issues and business operational risks.

The IT technician often ends up being the *kill-joy* that has to say this is more complicated that it first appears, and that it is not possible without extra expenditure & extra procedures to keep the company’s IT operations safe & secure.

There are a number of different ways to achieve Remote-Working. And each company needs to assess their own level of risk, decide what is appropriate expenditure & what safe-guards to put in place.

Doing something quick without the proper amount of consideration is risky and not advisable.

If you find that at the moment there is too much to consider in the rush to get it done, it would be wise to consider three pieces of advice :

1. For any employees that need long-term out-of-office IT functions
   a good approach is to allocate a corporate laptop to each of these employees and include them in the company's existing IT management procedures.

2. Carefully consider who is given the Remote-Working facility, as without strong IT data-controls in place then all Remote-Working employees need to be worthy of a high level of trust.

3. make Remote-Working a time-limited feature, and re-assess it again in a couple of months when times are less-rushed. Decide if Remote-Working is still necessary and worth the increased risks.
   If you do make the decision to keep Remote-Working, then put in place proper IT controls to reduce the chance of data-leakage & cyber-security problems.
   Finally, review the internet broadband package and '*right-size*' it to fits the needs of the whole company.

You can find out more by visiting : **www.fabric8n.com**

Steven Bishop

for Fabrication Systems

Email : steven.bishop @ fabric8n.com