Logical Solutions Security Paper

Logical Solutions is very aware of the business technology security uncertainty in the market. With this we have seen other providers using the FUD (Fear, Uncertainty and Doubt) tool to motivate customers to commit to projects.

We are often asked the question, what is security and how it can be defined?

> *"ICT Security is about protecting your **intellectual information**.*
> *The thing to remember is that security is a **Journey** and not a **Destination**"*

At Logical we believe in a *"real world"* approach to our customer's business security rather than an unrealistic theoretical approach. Security is a balancing act, working out how much security is appropriate for a specific customer and any special requirements needed, based on specific business applications the customer may have.

There are no quick fixes when it comes to security. It requires a change of mindset from the "just make it work" philosophy to, how to deliver that product or service in a way that would be difficult to compromise security objectives.

The most common cause of any security breach is human error, a good example of this is as follows.

"Sally, the part-time receptionist works two afternoons a week. As part of Sally's duties, the CEO has asked her to go and buy a new toaster for the lunchroom.

Sally wants to do a good job so buys the best toaster she can find. She has bought a toaster that can be connected to a Wi-Fi connection. Sally sets up the toaster and connects the toaster to the corporate wireless network with the details she has always used. "

Without knowing it Sally has compromised the IT security of your company by connecting an unknown device to your network. It is common for these types of devices to allow remote connectivity that could be used to access other network resources within your network. Your IT security procedure needs to accommodate situations like this. It would be great to think that all users would understand the shortfalls in Sally's actions but, very few users would give this a second thought.

The basis of security is to stop unwanted access to your corporate resources. In theory, this is simple, but situations like the above combined with users needing to be able to work from anywhere and everywhere makes this far more challenging in today's environment. Just securing your corporate network with a tricky firewall doesn't cut it any longer.

Information monitoring and processing is key to remaining secure. Having good monitoring solutions that identify behaviours outside the norm on your devices is paramount. In many cases your provider can configure automated actions.

Modern network devices produce detailed logs, but these logs are only useful when they are monitored and acted upon. SIEM (Security Information & Event Management) is a common tool that is used and can make decisions based on information from multiple devices at once, gaining a "big picture" overview of a environment rather than trying to make a decision based on information from a single device.

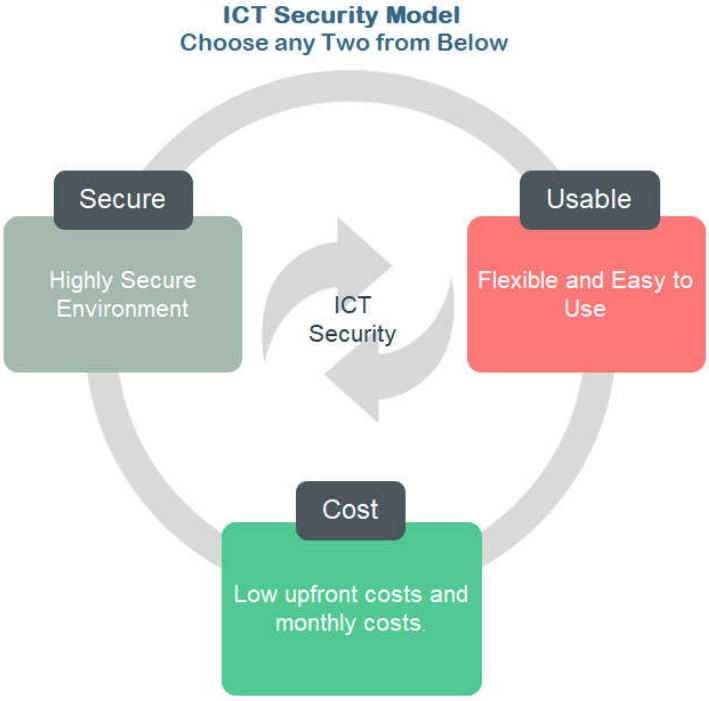
Another misconception is that Security is about complex user policies and procedures. While well-written policies can help, if no one ever reads or understands them they are ineffective.

Policies and procedures need to be simple and well understood by all. Staff buy-in is imperative to having successful security policies and procedures.

Bank and government departments spend hundreds of thousands on security and still, in many situations, can remain vulnerable. Your provider needs to look at your environment and understand the risk profile of your data and the best way to protect it.

Security is a balancing act, we need to balance the requirements of the customers business against the impact of security policies and also weigh up the finical impact of implementation and ongoing management.

One of the commonly used analogies is the "Security Triangle", Two of the three elements are achievable, but not all three.



Logical Solutions Security Assessment

The Logical Solutions security assessment is a five-step process. Each step in the process leads to the next step. By the end of the assessment, we should understand the requirements to secure your ICT environment.

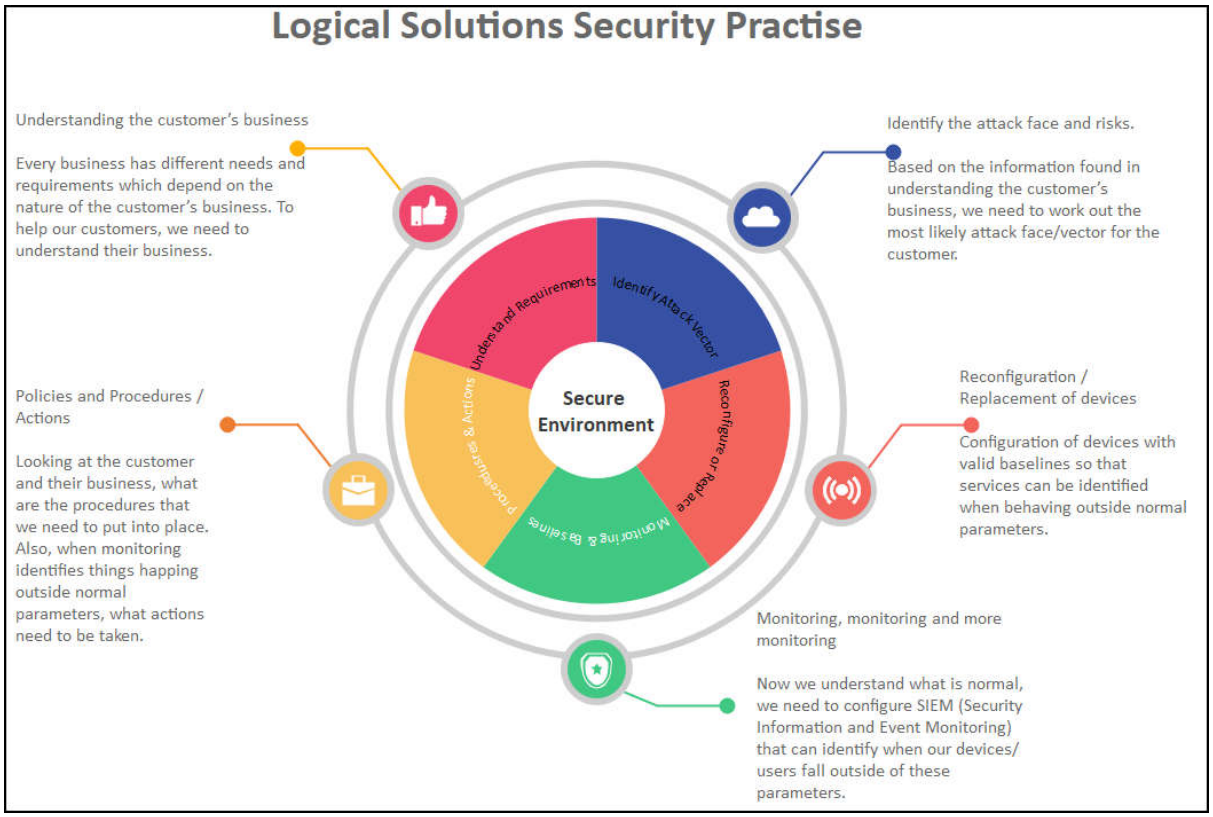
Firstly, we need to **understand your business**, what is the nature of your business and how does it use ICT to interact with its customers and suppliers?

Following on from this is to **identify the attack face**, understand the services as identified and look at how these services can become vulnerable. While you may have good security products in place, how have they been configured and what do they protect you from?

Configuration and replacement of dumb network hardware. To monitor your network hardware is required to provide information to a central system. Some of the lower cost "dumb" hardware is incapable of this. For hardware that is capable of this feature, it needs to be configured and tested.

monitor for attacks. It is as important to monitor failed attempts as well as successful attempts on your network. Baselines of network usage should be collected so that alerts can be configured to inform you when the network is operating outside normal parameters as this can be the sign of a larger issue.

Policies and procedures look at how to ensure your network remains secure. This section includes the "people element" and looks at behaviours in relation to your ICT platform. We also need to look at how to look at scenarios that can happen as part of monitoring or just day to day occurrences.



Questions and References

CERT is a website that has been created by the NZ Government to try and offer the businesses of NZ some security guidelines. One of the challenges facing business is not knowing who to believe when presented solutions. The site address is: https://www.cert.govt.nz/

At Logical Solutions, our security practice is closely aligned with the CERT guidelines and practices. Information is key to remaining secure and to that end we keep ourselves informed using information from multiple sources.

Over the last couple of years cloud-based technology has become more prevalent with customers. One of the most common challenges can be when software vendors "self-host" their applications. If the application is a web-based user interface, this makes sense. If the application is a "thick" application requiring a Terminal or RDS server is where we see problems.

These problems are both a security and usability issue. The usability issue is because the vendor based terminal server solution not being connected to your internal services. In most situations the vendor-based service is only a subset of what the business needs to run. This type of solution orphans' part of your environment and creates an additional unmanaged security zone.

The second issue is connectivity. If your vendor is asking you to make a direct RDP (Remote Desktop Protocol) connection across the internet without the use of some type of secure tunnelling, the connection is insecure. We see this often where customers are being told a direct connection is secured by restricting access to your network address. No matter what you are told, THIS IS INSECURE and shows a total lack of understanding about security. The only way to securely connect to an RDP connection across the internet is via a secure tunnel or VPN (Virtual Private Network)

Please see below references to this situation:

https://www.cert.govt.nz/business/guides/securing-your-internet-exposed-rdp-server/

Do you need to access the server itself?

In some cases, the RDP server is not even needed. For example, if you're using an RDP server to access applications remotely, you may choose to make the applications available directly over a VPN connection. Alternatively, you may choose to use modern virtual desktop products. These both serve as more secure alternatives to internet-exposed RDP.

Accessing Windows servers remotely, but more securely

If you need to access a Windows server from another network (for example staff working from home, or an IT service provider), we recommend using a VPN to create a tunnel between those networks.