Cyber Security Pointers

Cyber Security is a blanket term that covers a broad spectrum of ICT industry activities. Unfortunately, the term is often quoted with a presumption that you and I know the exact context, the relative importance and even the credibility of the person using the term.

This article is a simple guide for Local Government in WA.

What is Cyber Security?

It's important to understand that "Cyber Security" is not a prescriptive term – it is a *descriptive* term like "Cloud", "Digital Transformation", "Internet of Things" and "Single Point of Truth". As with these other terms, it describes a broad concept rather than an actual specifiable "thing". You can't just buy a "Cyber Security".

In a nutshell, Cyber Security has three inter-related but quite separate themes – Awareness, Defence and Recovery (or "What you know", "How you react" and "When you can get back on our feet after bad things have happened"). It's important to understand that threats to your cyber-security are not always malicious or deliberate and they are not always delivered from outside of your organisation. The one commonality is that these things can compromise the integrity of your digital access and assets – your "cyber" security if you will.

Awareness

This is simply *knowing* and/or *anticipating*.

Because threats are constantly changing and are a mix of direct, indirect and co-incidental events, it is almost impossible for anyone – even the security professionals – to fully keep up. At WALGA, we rely heavily on early notification tools such as ICT media, Security Bulletins, Industry events and credible marketing material for threat awareness. We rely on system reporting tools for component-stress and software alerts.

Our ICT team ensures that the entire WALGA staff is updated regularly, especially when either a new type of threat appears or when an existing threat is particularly active (eg shopping scams at Christmas, romance scams around Valentine's Day). Because malicious threats do not recognise traditional jurisdictional boundaries, our awareness needs to be global. Therefore, along with Australian resources, we also use the most globally aware companies for (free) advice.

Some of our members have seen a broader benefit in co-promoting "cyber" awareness to external businesses and individuals within their jurisdiction together with other bodies such as Education (eg online bullying, social media abuse), Chambers of Commerce (eg Fraud, Ransomware) and Police (eg money laundering, identity theft).

Internal, system or component threats should be managed using a pragmatic reporting, replacement and resource-appropriate regimen. It is much more effective to know in advance if, for example, a hard disk is showing signs of imminent failure or dangerous over-use than to simply respond after a failure. Keeping hardware and software components as contemporary as possible and reasonably un-stressed is an important risk mitigation strategy.

Defence

This is blocking or prevention **before** or **during** an event.

This area, along with Recovery, is the most saturated area of the technology market-place for "fix-it" products and services. It is arguably the area with most lies told and most under-delivered promises in the ICT industry today. The reality is that, no matter what products or services you purchase and/or implement for your Local Government, you should be aware that **there is no product or service available, at *any* cost, anywhere in the world that will totally eliminate the risk of cyber interference**. Notwithstanding this, many products do really well at mitigating one or more common risks. What is and isn't right for your local government is something that should be carefully considered and discussed with credible internal or external technology professionals. We would urge caution when dealing with vendors with a "fix-it" product wanting to give you (often "free") advice…

ICT professionals have been routinely mitigating risk of *systems* failure for decades using **resilience** (better quality components, uninterruptable power supplies, built-in failover techniques), **redundancy** (having physical duplication of independently capable key assets) and **rapid recovery** (having a "real-time" rebuild facility such as a database roll-back). These techniques have traditionally provided excellent prevention in the face of system failure and, in many cases, appear to be invisible to the broader organisation (other than budget, of course!).

Generally, professional ICT environments are built with "blocking" options purchased and enabled. This can range from system-wide blocking techniques such as forcing passwords to be a particular strength (different characters, minimum length etc) to intercepting, cleaning and de-spamming email (email filtering and virus protection) to selective blocking of incoming traffic (firewalls) through to desktop blocking techniques such as anti-virus and application-blocking (where an individual can't knowingly – or unknowingly – install or run unauthorised software).

In the WA Local Government context, some ICT environments have developed without the full benefit of consistent professional ICT advice or with limited "pay by the hour" ad hoc ICT advice. Local Governments without appropriate and contemporary blocking mechanisms coupled with inadequate system-failure mitigation magnify their risk of suffering a preventable outage.

Recovery

This is getting back on your feet **after** an event and is the true test of the effectiveness of your backup strategy, methodology and reliability. Note that this is more properly called Business *Resumption*, rather than Business *Continuity*. Business Continuity is what happens in the period *between* system failure and system resumption. It should deal with the Local Government's capacity to continue to provide selected day-to-day operations (without normal ICT systems).

For many cyber interruptions, getting back up and going is as simple as restarting systems and components (in the right order, of course!). Power or network outages and building compromise (flood, fire etc) can seriously compromise digital systems but, in most cases, it is relatively easy to restore operations immediately after the threat is removed or resolved.

Where there is a physical component involved, the recovery is usually almost as quick and painless, but the time to get the replacement component may add delays, especially for Local Governments with inherent delivery delays due to their locations in the state. If the component then needs to be configured or "properly" installed, the delay could be extended even further.

If a software component or data itself has suffered damage, recovery time will be largely determined by the availability and adequacy of system/application/data backups (aka digital copies of critical data). Time to recovery can range from (realistically) a full day to weeks to never. For specific single items, shorter recovery times *can* be possible (eg database roll-back, rebuild of a virtual machine etc) but Local Government Managers with responsibility for Risk Mitigation should be sceptical about stated, but untested, recovery times of less than a day. These promises are often based on "perfect world" assumptions for both the problem and the solution that rarely, if ever, exist.

In today's threat landscape, outright malicious damage is becoming rarer – mainly because there is no viable business case for simple destruction. Exceptions include sabotage by commercial competitors or damage by "hacktivists" that is designed to draw attention to a political or ethical situation. Theft of data (especially personally identifiable data or credit card credentials) is more common, as is targeted encryption (corruption) of data (Ransomware) and the deliberate choking of your ability to operate (Denial of Service). In a recent event, an email hosting service had its primary systems AND its backup systems *completely* destroyed, with the loss of *all* hosted email stores (ie – all of its customers' data). Ironically, one of the selling points for this service was the security of their system. In their case, recovery of their operations (and therefore their business) is unlikely to *ever* be achieved and the business will pay the ultimate price for poor data security practices (along with clearly inadequate defence).

Other cyber threats relate to systems-based fraudulent activity such as phantom employees, spurious invoices or requests for funding and spoofing (pretending to be someone or something by manipulating online credentials). The field of cyber-forensics deals with systemic issues such as these and, as with other crime scenes, the recommendation from experts is to report early and then don't interfere. If evidence has been (or *could* have been) subject to change, it greatly diminishes the chances of discovery and/or conviction.

Mitigation Options

Nothing can abrogate *your* responsibility for *your* data and systems. It can't be outsourced. However, some outsourceable practices can lower your risks.

Use of off-premise systems, software and data storage can allow for a much more sophisticated, deeply defended environment than is reasonably achievable by a single Local Government. So-called "cloud" offerings from reputable companies can offer the resilience; redundancy and rapid-recovery options required for a fraction of the cost of locally provided equivalents. "Cloud" also has the advantage that, if properly configured, it can remove your reliance on a single place or piece of equipment – so possibly a good choice where physical risk to infrastructure is high (consider risks posed by cyclones, bushfires, flooding, chemical spills, ammonium nitrate stockpiles etc) .

If using on-premise facilities, mitigate risk by purchasing infrastructure components with a level of quality commensurate with your risk appetite – there is a *big* difference between a $100 1Tb hard disk from a local electronics store and a $4,000 1Tb hard disk array from a specialist provider. Strive to maintain brand and model consistency in critical software, hardware and network components where appropriate. These items can be subject to significant changes or differences – and, despite the theoretical adoption of industry standards – do not all operate precisely the same. High impact ICT operations will almost always have a "preferred" provider. Care should be exercised when doing market comparisons because raw specifications rarely tell the full story about ICT components. Conversely, care should also be taken to ensure consistency (desirable) and complacency (undesirable) are fully understood by ICT and Procurement staff alike.

Partial mitigation for predictable component failure can be achieved by maintaining spares on site. Power transformers, hard disks and memory modules are examples of predictable failure points. Once again, the benefits of having consistent key infrastructure become self-evident when a single spare part can be used in multiple places.

BYC – Beyond Your Control

In 2018, more "cyber" or "digital" outages in Australia were caused by factors beyond the control of local ICT staff than *any* other form of attack. The three most common points of failure (and extended recovery delays) have been with Power, Network and Cloud Services – with all three intrinsically inter-dependent.

Mobile Phone, Data and Telephone services have all had widespread outages in Australia over the past two years. On a more localised level, quite lengthy power outages have occurred in all States. There have also been a number of high-profile data centre failures with significant impact. With the uptake of online services as a "first option", the risk of unexpected and unrecoverable outages of indeterminate time has increased. At a Local Government level, non-digital resilience can be required (eg, I should be able to get my dog out of the pound – even if digital systems are down) and local Disaster Recovery plans should anticipate the risk of a temporary but *total* loss of data services.

The use of Uninterruptable Power Supplies (UPSs) in most operational contexts is to avoid small (<4 hours) outages and to filter incoming power so that it is delivered safely to electronic components. Where the requirement for longer-term uninterruptable power supply exists, the use of ancillary generators is the most common approach taken. Even if Local Governments take this (expensive) option, a broader power outage could still cause upstream failures. In WA, many communities do *not* have truly redundant power reticulation (ie more than one path from generation to consumption points).

The last element that is beyond your control is the "organic interface" – your human staff and constituents. Many of the Cyber threats prevalent today are based on centuries-old human attributes such as greed, fear and gullibility. Education is your most valuable tool in this regard. Along with subjects such as Workplace Safety, Mixed Abilities, Fire Prevention, Cultural Awareness and other well-established awareness programs in Local Government, Cyber Awareness should be on your regular agenda.

Assume your Local Government is *already* subject to cyber-attack of one sort or another and presume you will continue to be exposed to more frequent and more sophisticated attacks into the future. Digital incursions and any resulting damage is important to counter (Cyber Security) but having the ability to recover gracefully and fully after an event is even *more* important. The former is largely beyond your control but the latter is absolutely a choice. Your choice.

More information

WALGA has a number of reputable providers on its ICT & Related Preferred Supplier panel that can offer management, operational or holistic consultancy services and products to help secure your Cyber assets. Because your cyber security has many facets, so too do our PSA lists.

For more information, we recommend looking to the broad array of resources published through the academic, government and commercial sectors at a statewide, national and global level. Awareness material, which can also include good practice guidance, is often free. Defence and Recovery tools, on the other hand, can be quite expensive and there is definitely not a "one size fits all" solution. Use of credible consultants to help you decide what are the most fit-for-purpose tools for your LG is a good strategy.

Here are some links that you might find helpful for further research. It is by no means exhaustive so we encourage you to seek more advice to suit your specific circumstances and interest.

Government

The Australian Cyber Security Centre	https://acsc.gov.au/
ACCC Scam watch	https://www.scamwatch.gov.au/
WA ScamNet	http://www.scamnet.wa.gov.au/scamnet/
ACORN	https://www.acorn.gov.au/
FBI	https://www.fbi.gov/investigate/cyber
Australian Institute of Criminology	https://aic.gov.au/

Industry

Akamai	https://www.akamai.com
Symantec	https://www.symantec.com/
Sophos	https://www.sophos.com/en-us.aspx
Secureworks (DELL)	https://www.secureworks.com.au/
DELL/EMC	https://www.dellemc.com/en-us/data-protection/
Microsoft	https://www.microsoft.com/en-us/security

Academic

ECU	http://www.ecu.edu.au/degrees/study-areas/science/cyber-security
Monash	https://www.monash.edu/cybersecurity-lab

For further information, please contact Peter Johnson, the ICT Manager at WALGA at ictmanager@walga.asn.au