Case study – Legacy Systems

You can't teach an old dog new tricks

No one likes debt, especially "technology debt". You know, those systems you just can't seem to get rid of in your environment despite how out of support, expensive to maintain and people dependent they are? But we all know that leaving them around is just a ticking time bomb and managing them out of the environment proactively – regardless of how challenging – is still a better position to be in than trying to do so under the duress of an incident, such as the one the Department of Innovation comes to experience…

Synopsis

The Department of Innovation was using a legacy system to extract data and produce reports that provided mission critical information about the innovation projects the department was managing. Workers had been complaining about a number of faults with the legacy reporting system. IT claimed that vendor support was no longer available for the system, and patches were infrequent and costly. The system is a key dependency to the critical business activity of reporting, despite being known as out of date by the user base. No integration between the source data systems and the reporting capability currently existed.

Furthermore, there was only one person in the organisation who knew how to manage the system. The legacy system was difficult to backup and recover. Ransomware hit the department and the data residing on the legacy system was no longer accessible. With no redundancy options, no way to recover and the only person who understood the environment away, the department found itself in a bind.

Background

“In summary, it’s pretty obvious that we need to migrate off our legacy system, there are a number of reasons why – patching is infrequent as the system is ‘out of support’ with the vendor; there’s too much dependency on one person to manage the system; and there are many functional limitations. I suggest we adopt one of the newer aforementioned systems as a solution.” Theo said as he wrapped up his presentation to a round of applause from management. He was hoping this time he put forward a more compelling case as management were unperturbed when they dismissed his last case. This time he’d established consensus on the key issues and risks with the system owners and users. “Theo – we understand your rationale behind this business case and those are all valid points … but we simply feel that the operational risk of migrating from the existing system is too high and we can’t afford an outage or lengthy migration process. Not to mention it’s costly for the business” [1], said Humphrey Boxhugger– the IT infrastructure manager. “We need to keep our costs down and come in on budget. We don’t have adequate funding. Besides, if it’s still delivering the required business outcomes, is there really a need to invest right now?” Conceding to management, Theo threw up his hands, as he’d done all he could to highlight the need for an updated reporting system.

Just another day in IT…

By all accounts it seemed to be a normal Monday morning as Theo Kalipraxi, systems administrator (reporting system), strolled into the office with his coffee. For some unknown reason his stomach felt strange. He soon understood why as he stepped off the lift onto IT’s floor. Sharon Stitch, a system support officer, was there waiting for him, “Theo we have another incident with the reporting system, we’ve been getting calls and tickets raised all morning. The system is down for some reason, and James Forsithe (service delivery manager), needs you in the incident meeting.” When Theo got to the meeting several avenues of discussion were underway on how to best resolve this issue. “Patching the system would be the best bet, but it’s hard to get a proper patch in place in such a short time frame given the system is out of vendor support. Since we also don’t have in house support to handle this, we’ll need to ask the vendor to develop a customised solution to prevent any further impact to us.” said Theo. After discussing on the phone with the vendor and diagnosing the issue, he found that it could take up to a week to get this fixed and it would be quite expensive, since the vendor needed to deploy a special team to fix what appeared to be a complex issue. After stressing for a few hours, the team agreed in the interim to issue workaround instructions to users via email.

From one adventure to another

On Friday (relieved to take a break from work), Theo went on long service leave, and as he switched to holiday mode, he packed his bags to climb Mt Kilimanjaro where adventure was waiting. Back at the department, users had been using the reporting system with the workaround instructions from the email earlier in the week, and Jenny Snapbook in marketing was suddenly unable to access the reporting system. When she launched it, she was greeted with a ransomware demand for 2 Bitcoin within 48 hours. She confirmed that her colleagues were also experiencing the same issue. The IT department, who were now aware of the threat, made attempts to recover the data from backups but were unsuccessful due to inherent issues with the system [2]. SDM James asked the following question - “So who do we have from a system management perspective to assist with resolving this?” After they realised nobody had the skillset to assist with system management [3], the organisation faced an outage that seriously impacted the delivery of services. Whilst critical reporting was not being performed at the ideal level, a manual workaround was issued. Subsequently, given that it was also late Friday afternoon and the team had some comfort the ransomware was contained to a single system, it was decided that the issue could be left until Monday.

Risk it for the biscuit

Back on Monday morning, the ransom had increased to 4 Bitcoin, with an added threat to delete all data within the system if the ransom was not met. The Department of Innovation had never encountered ransomware in the department before and didn't have a great amount of knowledge or confidence to deal with it 🚩[4]. As a result, they didn't fully understand the scope of the incident. Nonetheless, the team attempted to resolve the issue alone. During the incident meeting someone asked "Even if we pay the ransom, we may not get all our data back. But if we don't pay it, we are at risk of having our data deleted. While we know government organisations aren't supposed to pay a ransom, what choice do we have?" Backed into a corner, the IT team suggested that management pay the ransom in the hope they would get their system back to normal.

An expensive lesson – from bad to worse

After almost an entire week of system outage, the department escalated to Theo. As he was away on holiday, unaware of the events, he did not return their call. The business paid the ransom, but this failed to resolve the problem. They were forced to spend more money in recovery processes, and then a remediation program to migrate to a new system, and until this was completed the outage continued. It appeared the incident was over, but senior management still wanted to understand what caused it, and what the overall impact was to the business. Humphrey explained to Sarah Jennings, Chief Information Officer: "During the ransom, users had to resort to manual reporting methods – which was better than nothing, however, this meant that the business was deprived of timely insights. Our post-incident review revealed that the reporting system had a number of issues from a security standpoint" 🚩[5]. Sarah understood that the impacts of this incident were yet to be fully recognised, and still had the potential to harm them in a variety of ways from a financial, legal, and reputational standpoint. For more clarity, she hired forensic experts to research the origins the ransomware. She planned to claim the cost of this on the company's cyber insurance, in addition to the ransom that was paid. She also notified the Office of the Victorian Information Commissioner (OVIC) of the information security incident related to the availability to critical business information, as required under the Victorian Protective Data Security Standards. Upon advising that the risk register be updated, she reflected with Humphrey that "Ultimately, our lack of proper management of the system has meant that we've funded cybercriminal behaviour by paying the ransom, and has ended up costing us more than if we'd just migrated off the legacy system in the first place."

Conclusion

Legacy systems pose several issues for organisations and are well known areas of information security weakness. Organisations still using legacy systems / technology may be opening themselves up to business (including security) risks. These include operational inefficiencies and a reduction in effective business processes. Users of these legacy systems and technology may be forced to use outdated features or reduced functionality. Some organisations may face high maintenance costs for their legacy systems / technology. These costs may be reduced by implementing newer technologies which would also help mitigate some of the security risks posed to the organisation (i.e. unsupported, unpatched).

The facts

This case study was inspired by real events, and Victorian public sector organisations still using legacy systems experience an array of challenges when it comes to maintaining this system. Often, maintaining a legacy system imposes significant inefficiencies (including cost) on organisations.

An example of legacy systems can be found here:

https://www.itnews.com.au/news/leap-replacement-drops-off-victoria-polices-agenda-419277

Impacts of legacy systems

What was affected	Impact
Service Delivery	Information required to assist in the day to day functioning of the department was not available. This led to productivity issues, missed deadlines and ultimately, the cost of paying the ransom.
Reputation	If criminal activity enablement (i.e. paying a ransom) is associated with a Victorian public sector organisation, this is not only embarrassing for the organisation, but also reduces public trust from the local community. In turn, this creates a new barrier when engaging with the community.

Alignment to risk

'The risk of ….event…. **caused by** ….how…. **resulting in** ….impact(s)…'.

This case study may manifest itself as the following risk statements in an organisation's risk register:

1. The risk of	2. Caused by	3. Resulting in
Unavailability of the department's critical reporting information on the legacy reporting system	Cybercriminals launching a ransomware attack	Degradation of service delivery and reputational damage
Compromise to the integrity of reporting information from reduced ability to operate the reporting system and process reporting information completely and accurately	The unavailability of key resources (e.g. system manager)	Operational inefficiency, ineffective decision-making and negative financial impact

Improper allocation of financial resources	The unsustainable cost of maintaining the legacy reporting system	Negative financial impact

Key flags 🚩 and control considerations

Flag	Issue	Control considerations	Element reference
1	Understanding and managing the lifecycle of ICT assets.	Understanding how to best manage the lifecycle of ICT assets including managing legacy systems out of the environment is important for the organisation to manage productivity and risk. Additionally, introducing an SOE for all key systems including a strong focus on end user devices allows those systems to be less "exploitable" to attacks (such as the loading of malware should a user click on a phishing link). *Standard 11 – Information Communications Technology (ICT) Security: E11.020, E11.090*	*E11.020* - The organisation manages all ICT assets (e.g., on-site and off-site) throughout their lifecycle. *E11.090* – The organisation manages standard operating environments (SOEs) for all ICT assets, including end user access devices (workstations, mobile phones, laptops), network infrastructure, servers and Internet of Things (IoT) commensurate with security risk.

Flag	Issue	Control considerations	Element reference
2	Regular testing of disaster recovery processes.	Undertaking regular testing of key information security aspects of business continuity and disaster recovery can help ensure that the impact of disruption can be better managed. *Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery: E7.030* *Standard 11 – Information Communications Technology (ICT) Security: E11.180*	*E7.030* – The organisation regularly tests (at least annually) its business continuity and disaster recovery plan(s). *E11.180* - The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).

3	Identifying gaps in roles and responsibilities especially where there are single point of dependencies.	Having visibility of processes and roles/responsibilities allows gaps to be identified that may contribute to increased impact of business disruption. This includes identifying key personnel dependencies and how best to manage them. To further minimise the likelihood of attacks like phishing attempts being successful, the organisation implements a security user awareness program that includes a strong focus on phishing-based attacks and how to identify them. *Standard 3 – Information Security Risk Management: E3.010* *Standard 4 – Information Access: E4.010, E4.020, E4.040* *Standard 5 – Information Security Obligations: E5.030*	*E3.010* – The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: • Risk identification; • Risk analysis; • Risk evaluation; and • Risk treatment. *E4.010* – The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know. *E4.020* – The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information. *E4.040* - The organisation implements logical access controls (e.g., network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know. *E5.030* – The organisation delivers information security training and awareness to all persons with access to public

Flag	Issue	Control considerations	Element reference
			sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.
4	Having appropriate information security incident management processes.	Information Security Incident Management within the organisation should factor in the five phases and include specific operating procedures and testing of scenarios/use cases that are common and/or high risk as assessed by the organisation. *Standard 6 – Information Security Incident Management: E6.030*	*E6.030* - The organisation's information security incident management processes and plan(s) contain the five phases of: • Plan and prepare; • Detect and report; • Assess and decide; • Respond (contain, eradicate, recover, notify); and • Lessons learnt.
5	Identification and management of vulnerabilities of key ICT assets.	ICT assets, including those that are legacy, require timely identification of vulnerabilities and a remediation approach (which may include compensating controls) to limit the likelihood of vulnerabilities from being exploited. *Standard 11 – Information Communications Technology (ICT) Security: E11.040*	*E11.040* - The organisation undertakes risk-prioritised vulnerability management activities (e.g. patch management, penetration testing, continuous monitoring systems).

Suggested next steps

Implementation or uplift of controls covering:

- **Lifecycle management of ICT assets** – ensuring that appropriate project plans are in place to migrate from legacy based systems, especially those that are difficult to support, manage and secure;
- **Business continuity and disaster recovery processes –** ensuring that appropriate policies and processes are in place to manage business disruption and regularly testing them so they can operate effectively when most needed;
- **Identifying single points of failure** – ensuring that any single point of failure within the organisation is identified (not just system, but also people and processes) so appropriate planning and management is in place to minimise risk; and
- **Incident management** – ensuring that suitable standard operating procedures are in place for the handling of information security related incidents so incidents can be managed as efficiently as possible – therefore minimising the impact to the organisation.

More information

Contact OVIC at security@ovic.vic.gov.au if you would like to discuss this case study further.

Further Information

Contact Us

t: 1300 00 6842
e: security@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

This case study does not constitute legal advice and should not be used as a substitute for applying the provisions of the Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.

Please note that the events depicted in this case study are based on actual events, however the characters are purely fictional and any similarity to any person living or dead is merely coincidental.