getKambium

Louie BTR Review 2022

Prepared By:	Testing Company
For:	Louie One
Author:	Rhys Kerrigan
Date:	2022-10-06
Document Reference:	Louie BTR Review 2022
Version:	1.0

Executive Summary

Louie One have identified that, to be competitive, their staff need IT systems that are collaborative, reliable, and secure. To support this vision, Testing Company have reviewed the current technology systems and processes in place at Louie One and put together a plan of recommendations to make the IT systems better suited to the way that Louie One staff work.

This document outlines the results of work done by Rhys Kerrigan from Testing Company and Jane Doe from Louie One in September 2022 to understand their business objectives through the questions in the GetKambium Business Technology Review process.

Louie One have some good practices and systems in place, however further should be undertaken to reduce the risk of security threats, and to streamline manufacturing processes.

We recommend that Louie One continue to focus on how technology can work for their staff to help achieve their goals. Areas of note include:

1. Better manage and protect your critical information assets.
2. Reduce risk and data loss by improving security measures.
3. Apply governance controls through updated policies and processes.
4. Improve your business and staff resiliency and readiness for major events and disruption.
5. Implement technology changes that add real value to your staff and business.

This document outlines a proposed roadmap to implement the recommendations found and outlines some broader strategies. The document is broken into six sections:

1. This Executive Summary.
2. The Current State outlining our understanding of the organization, systems, issues and projects at Louie One.
3. A Strategy with Priorities and a Roadmap for Louie One.
4. The Recommendation Summary that illustrates the business benefit of the recommendations and reference index.
5. A Financial projection of the current IT costs and implementation costs of the Recommendations.
6. The details of the Recommendations, sorted into 'Must Do', 'Should Do' and 'Could Do'.

Current State

What we understand your company does:

Make beverages

What makes your company successful?

The beverages are really tasty

Internal company changes and challenges

Adding new production facility in Florida

External market and industry changes:

Big players taking over the market

Current IT funding structure:

CFO controls IT budget and is decision maker. Internal IT support team with out-sourced IT support

Office Locations:

Tampa, Auckland, London

3
IT Staff

350
Total Staff Employed

0
Contractor Staff

4
Key Applications

3
Client Identified Issues

2
Current or Planned Projects

Key Systems

Application	Purpose	Hosting	Monthly Cost
SalesForce	CRM	SaaS	450.00
NetSuite	Financials	SaaS	600.00
BevBuilder	Manufacturing process	On-premise	0.00
ProMapp	Process mapping	SaaS	250.00

Client Identified Issues

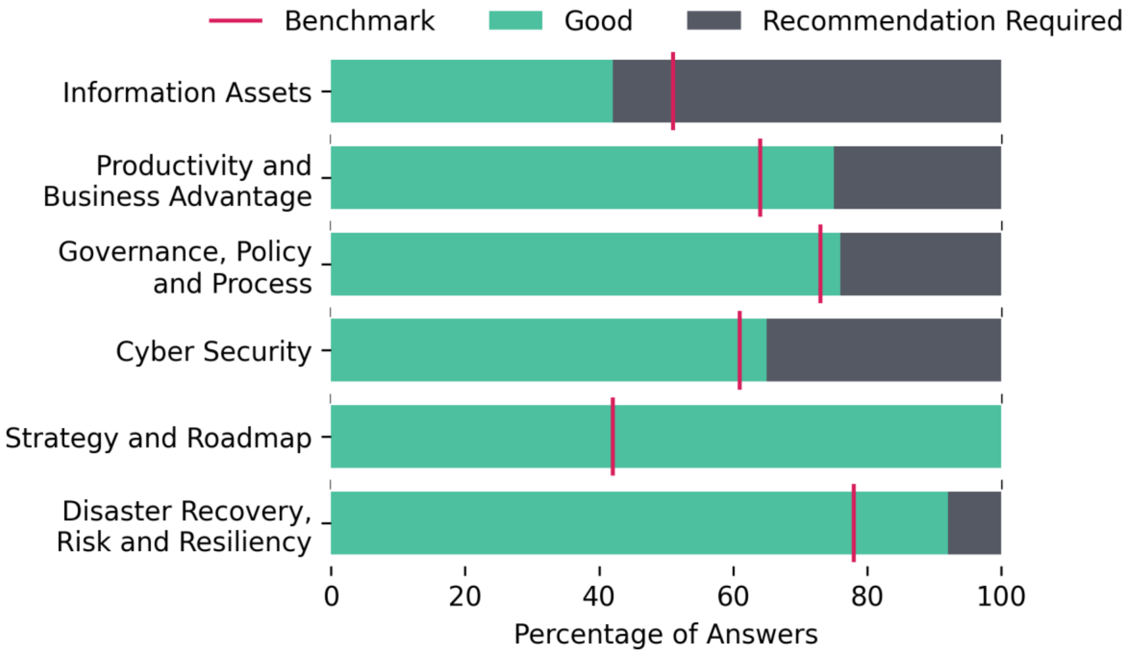
Issue or Risk	Concern
Security concerns	High
Company data on personal drives	High
Improved MRP application could help business	Medium

Current and Planned Projects

Project	Timeframe	Setup Cost	Monthly Cost
Implement MFA	Within 3 months	1500.00	150.00
Move to Cloud PBX	Within 12 months	25000.00	1200.00

Questionnaire Summary

The following graph outlines the current state of Louie One in the various categories measured. The benchmarks show the current average response across all completed reviews.



Strategy

Key Themes

1. Better manage and protect your critical information assets.

- Computer hardware rotation
- Emerging technology
- Key applications

2. Reduce risk and data loss by improving security measures.

- Physical Security Review
- User Account Audit
- Staff cyber security awareness

3. Apply governance controls through updated policies and processes.

- IT Policies
- IT changes linked to HR or payroll

4. Improve your business and staff resiliency and readiness for major events and disruption.

- Disaster Recovery Plan

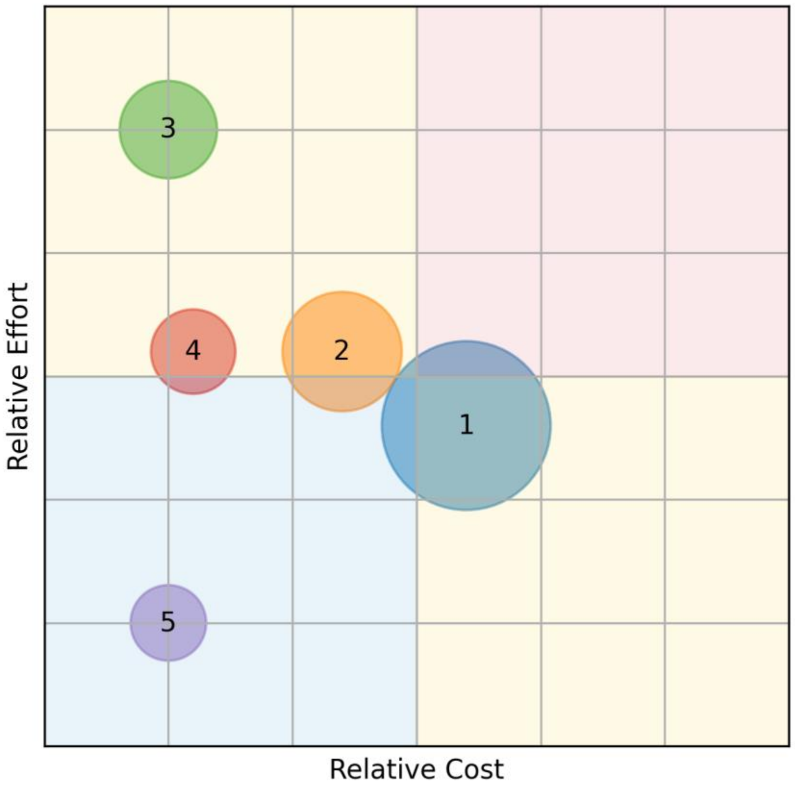
5. Implement technology changes that add real value to your staff and business.

- Effective Remote Working
- Company communication

Priorities

The graph below summarizes the priority, and relative cost and effort of the review's key strategies. Priority is indicated by bubble size, and cost and effort are the horizontal and vertical axes, respectively.

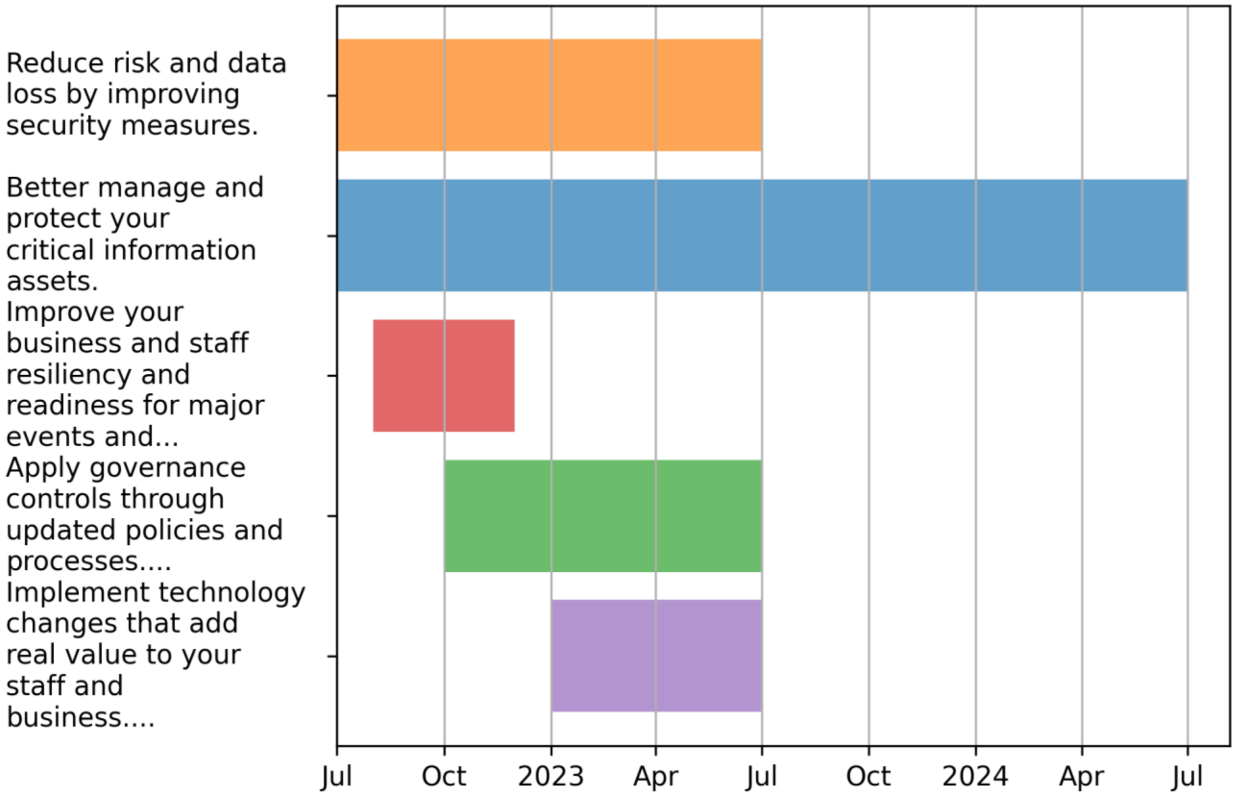
Bubbles in the chart that are large (high priority) and in the bottom left quadrant (low cost and effort) are more easily addressed and will have a high business benefit.



1. Better manage and protect your critical information assets.
2. Reduce risk and data loss by improving security measures.
3. Apply governance controls through updated policies and processes.
4. Improve your business and staff resiliency and readiness for major events and disruption.
5. Implement technology changes that add real value to your staff and business.

Roadmap

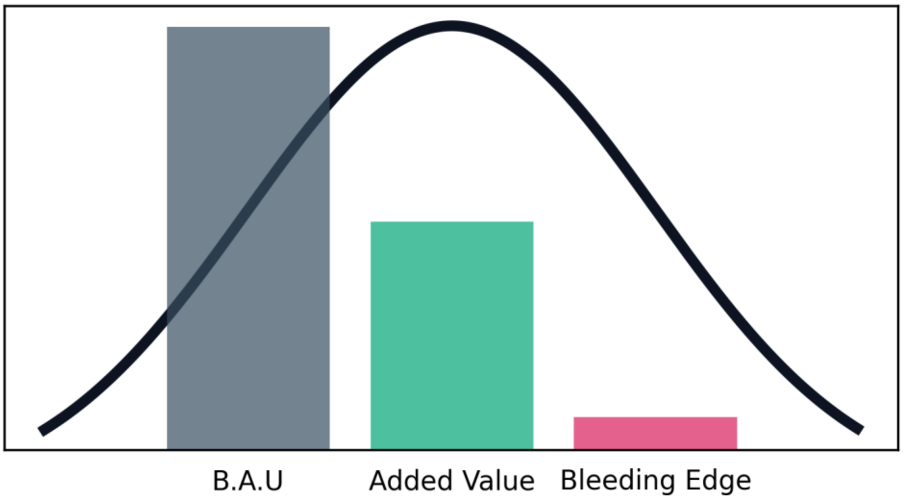
The graph below provides a guideline on how best to implement the Strategy and an indication of the timeframes involved.



Recommendation Summary

Business Benefit

The following graph maps the "business benefit" of each recommendation into the groups "Business as Usual", "Added Value" and "Bleeding Edge". The bell curve overlay indicates the ideal scenario, with most effort going into adding value.



Recommendation Index

The following tables outline an index of all recommendations. Note that all costs are approximate. The approximate effort required to implement the recommendation is given as an indication only of the work involved/complexity of the task.

Must Do

Title	Effort/Cost	Business Benefit
Information asset protection	1 - 2 Weeks	Business As Usual
Regulatory requirements	1 - 2 Days, $2,500 - $2,500 one-off	Business As Usual
IT changes linked to HR or payroll	2 - 4 Hours	Business As Usual
Data Privacy Policy	3 - 4 Days, $3,500 - $4,500 one-off	Business As Usual
Business Intelligence and Reporting	2 - 3 Weeks, $150 - $450 p/a	Added Value
Incident Response Plan and Playbooks	2 - 3 Days, $4,000 - $6,000 one-off	Business As Usual
Cyber Insurance	1 - 2 Days, $10,000 - $20,000 p/a	Business As Usual
Disaster Recovery Plan	1 - 2 Weeks, $10,000 - $20,000 one-off	Business As Usual

Should Do

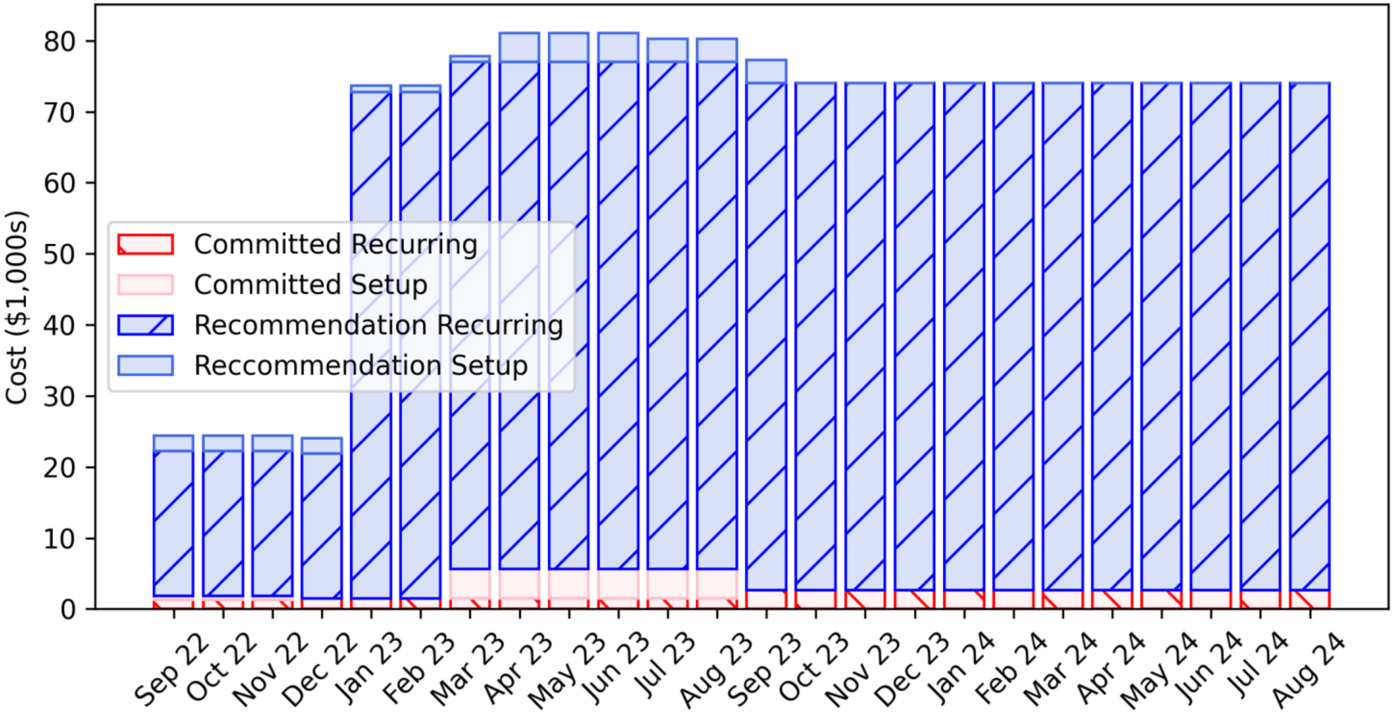
Title	Effort/Cost	Business Benefit
Key applications	2 - 4 Months	Added Value
Finding and Saving information	1 - 2 Weeks	Added Value
Drive Encryption	3 - 5 Days	Business As Usual
User Account Audit	6 - 8 Hours	Business As Usual
Staff cyber security awareness	1 - 2 Days, $500 - $750 p/m	Added Value
Financial transaction security	1 - 2 Days, $100 - $150 p/m	Business As Usual
IT Policies	2 - 3 Days	Business As Usual
Business Process Efficiency	1 - 2 Weeks	Added Value
Company communication	1 - 2 Days	Added Value

Could Do

Title	Effort/Cost	Business Benefit
Computer hardware rotation	2 - 3 Days, $40,000 - $50,000 p/a	Added Value
Emerging technology	1 - 2 Days	Bleeding Edge
Effective Remote Working	4 - 5 Days	Business As Usual
Physical Security Review	3 - 4 Days, $3,500 - $5,000 one-off	Business As Usual

Financial

Financial Summary



The Financial chart aggregates your committed costs (red), which comprise existing key applications, and current and planned project costs. The estimated costs for Recommendations are displayed in blue. The costs are further broken down into setup/one-off costs (solid) and recurring/monthly costs (striped). The chart assumes the setup/one-off costs are spread evenly throughout the implementation period of the project or Recommendation.

Financial Detail

1 Year Projected Committed Costs

Expense	Sep 22	Oct 22	Nov 22	Dec 22	Jan 23	Feb 23	Mar 23	Apr 23	May 23	Jun 23	Jul 23	Aug 23
SalesForce	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00
NetSuite	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00
BevBuilder												
ProMapp	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00
Implement MFA	500.00	500.00	500.00	150.00	150.00	150.00	150.00	150.00	150.00	150.00	150.00	150.00
Move to Cloud PBX							4166.67	4166.67	4166.67	4166.67	4166.67	4166.67

1 Year Projected Recommendation Costs

Recommendation	Sep 22	Oct 22	Nov 22	Dec 22	Jan 23	Feb 23	Mar 23	Apr 23	May 23	Jun 23	Jul 23	Aug 23
Computer hardware rotation					50000.00	50000.00	50000.00	50000.00	50000.00	50000.00	50000.00	50000.00
Emerging technology												
Effective Remote Working												
Physical Security Review					828.73	828.73	828.73	828.73	828.73	828.73		
Key applications												
Finding and Saving information												
Drive Encryption												

User Account Audit												
Staff cyber security awareness					750.00	750.00	750.00	750.00	750.00	750.00	750.00	750.00
Financial transaction security					150.00	150.00	150.00	150.00	150.00	150.00	150.00	150.00
IT Policies												
Business Process Efficiency												
Company communication												
Information asset protection												
Regulatory requirements	407.61	407.61	407.61	407.61								
IT changes linked to HR or payroll												
Data Privacy Policy	733.70	733.70	733.70	733.70								
Business Intelligence and Reporting	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00	450.00
Incident Response Plan and Playbooks	978.26	978.26	978.26	978.26								
Cyber Insurance	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00	20000.00
Disaster Recovery Plan								3278.69	3278.69	3278.69	3278.69	3278.69

Recommendations

Must Do

Information Assets - Information asset protection

Business Problem

What information assets do you have? Do you know where your data is stored? Not just digital. These could be HR or client records. Where/how are they stored? What is the impact of your information being lost/corrupted/encrypted or put in a competitor's hands? Do you have a "secret sauce" or recipe or other critical intellectual property? Do you know who has access to the critical information currently?

How often do you assess whether your information assets are protected?

Technologies, such as "data leakage prevention" (DLP) or "information rights management" (IRM) can help protect this sensitive information.

To keep your networks secure, you need to know about everything that’s in use on them. Sometimes people add their own software, or login to web-based applications without getting authorization or letting the IT team know. This is called “Shadow IT.” Usually, it’s people trying to do their jobs in what they think is a responsible way; there’s a task they need to do, and there isn’t already a company tool available for it, or they don’t know there is. By logging into these applications they could be exposing sensitive company or personal information without the IT team being aware of it.

Current Situation

Worried about data on personal staff drives and services

Recommendation

We recommend two steps to better understand your Information Assets and how they are protected:

1. Review the server and cloud data and permissions in place currently. Document who has access to what files and folders currently and review these permissions with the appropriate staff. Update the permissions as required.

2. Confirm what business critical data you have, where it is and who uses it. Then investigate ways to better protect this data as required. Solutions such as Information Rights Management (IRM) from Office 365 or Data Leakage Prevention (DLP) may be able to help.

We recommend reiterating with staff that there is a company cloud storage solution in place and they should use it instead of personal versions.

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 1 - 2 Weeks

Information Assets - Regulatory requirements

Business Problem

Certain industries or companies have regulatory requirements that impact the way in which data is stored or the IT infrastructure is configured. For example, any company that stores credit card information must meet PCI DSS standards, and any company that stores patient medical information must meet standards set by Ministry of Health / Department of Health.

Current Situation

Need to review this, not one recently

Recommendation

Further steps should be put in place to investigate and document the regulatory requirements that effect your organization, and then steps taken to implement the requirements.

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 1 - 2 Days, $2,500 - $2,500 one-off

Governance, Policy and Process - IT changes linked to HR or payroll

Business Problem

Often the IT team are the last people to know when new staff start, staff leave or change roles. This runs the risk of disruption to the staff member, or (worse) staff incorrectly having access to company information after they have left or changed roles. Linking these processes to HR or payroll provides a repeatable procedure for people starting and leaving ensure that access setup is consistent, and removed when staff leave. It also allows IT to be made aware of changes well in advance of the change occurring.

Current Situation

Not currently - exit policy needs to be improved

Recommendation

We recommend that the exit procedure for when users leave is formalized so that the IT team is informed in a timely manner. This could be tied in with the payroll personnel so they let IT know when a person has left, or tied in with the property managers so that when security access cards are returned, IT is notified.

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 2 - 4 Hours

Information Assets - Data Privacy Policy

Business Problem

Data privacy regulations have been strengthened in many countries - driven largely by the "GDPR" regulations in Europe.

These regulations typically enforce notifying authorities and users when a data breach has occurred - and large penalties if you don't notify in a specific time-frame.

You should have a privacy policy and consider what personal information you store - both your customers and your staff.

For example, do you store HR records for staff that have left? Would they have a reasonable expectation that you have deleted this?

Current Situation

No distinct privacy policy in place. Some factors covered off in company policy.

Recommendation

We recommend that a data privacy policy is created based on best practice and research performed across the industry. Staff should be trained on the privacy policy and it should be included in the staff induction process. The public websites should have updated consent boxes.

- Build customer trust
- Improve brand image and reputation
- Improve data governance
- Improve information security
- Improve competitive advantage

To create a data privacy policy the following areas and questions need to be answered:

- What data do we hold?
- We don’t tend to delete data – why do we hold it?
- When, if at all, should we purge it? Why?
- If someone asks us, what is our process on checking they are how they say they are?
- How would we know if it were stolen or leaked? Who would we notify?
- What is our obligation to the clients and their staff? Is it different?
- Who do we notify?

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 3 - 4 Days, $3,500 - $4,500 one-off

Information Assets - Business Intelligence and Reporting

Business Problem

Companies use Business Intelligence (BI) to detect significant events and identify/monitor business trends in order to adapt quickly to their changing environment. Effective BI and reporting can:

- Gain insights into staff and customer behavior
- To improve visibility of trends
- To turn data into actionable information
- To improve efficiency
- To gain competitive advantage

Current Situation

No dashboarding in the production warehouse

Recommendation

We recommend investigating a more dynamic BI tool for certain staff to have access to so they can have more dynamic access to the data, and hopefully reduce the impact on IT. The BI tool implemented should be fit for purpose for the staff that use it. For example, large screen dashboards may be useful in a warehouse or call center to provide visibility of production KPIs, but a PowerBI app on a mobile device may be better suited to sales people who want to dynamically slice data that is relevant to them.

Business Benefit: Added Value

Timeframe: Jul-22 - Jan-23

Cost/Effort: 2 - 3 Weeks, $150 - $450 p/a

Cyber Security - Incident Response Plan and Playbooks

Business Problem

It is critical that every business can identify and respond to a security incident or event. Damage to reputation, revenue, and customer trust are tangible risks businesses need to mitigate in the event they become a victim of the latest cyber-attack.

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyber-attack. The Response Plan and Playbook, is what defines a breach, the roles and responsibilities of the security team, tools for managing a breach, steps that will need to be taken to address a security incident, how the incident will be investigated and communicated, and the notification requirements following a data breach.

Current Situation

Part of DR plan - needs reviewing

Recommendation

We recommend that an Incident Response Plan and adjoining Incident Response Playbook are created and maintained. Incident response is about making and having a flight plan before it becomes necessary. Rather than just being an IT-centric process, it is an overall business function that helps ensure an organization can make quick decisions with reliable information. Not only are technical staff from the IT and security departments involved, so too are representatives from other core aspects of the business.

Creating an Incident Response Plan and Playbook, may involve the following steps:

- Understand what might put your business at risk
- Create a security risk and incident triage matrix
- Determine the risk scales and responses required
- Establish roles and responsibilities
- Create the Playbook – Should contain these 7 core steps

1. Prepare
2. Detect
3. Analyse
4. Contain
5. Eradicate
6. Recover
7. Post-Incident Handling

- Align or write/update IT Policies to correspond with changes
- Communicate the plan
- Educate your employees
- Test your plan

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 2 - 3 Days, $4,000 - $6,000 one-off

Cyber Security - Cyber Insurance

Business Problem

Any business that uses any kind of technology for its operations, whether in the cloud or on premise servers and devices, could face potential cyber risks. In todays digital world and with the current sophistication and organized approach of cyber criminals, it is highly likely that businesses will have to deal with a breach at some stage.

Having Cyber Insurance is paramount in helping businesses recover from a cyber-attack, that could cause disruption to a company's ability to generate revenue in the light of company data loss, IT services taken off line, or confidential information stolen through a privacy breach and thus reputation loss.

Equally as valuable are the results of the Cyber Audits that go hand in hand with obtaining Cyber Insurance. Continuous improvement is greatly improved if your business is proactive about implementing the recommendations and best practice suggestions produced as a result of these audits.

Current Situation

Not in place

Recommendation

We recommend that you engage with a broker to secure Cyber Insurance for your business.

A robust Cyber Insurance policy should include basic cover for ransomware, privacy breaches, re-writing of lost records and the transmissions of a computer virus.

Broader policies may also include:

- Loss of business income
- Forensic costs to determine the extent of the event
- Extortion costs incurred in the threat of an event or a ransomware assault
- Costs to restore the network
- Public relations costs to minimize reputational damage

More common policies are now also focused on privacy breaches and the covering of 3rd party costs that your business may be liable for. This is especially important if you collect, store or transmit any personal, private, financial or health information.

These policies may cover:

- Regulatory fines and penalties
- Third-party damages
- Public relations costs
- Forensics costs
- Claims for compensation from customers or other third parties such as banks or suppliers
- Costs of investigations instigated by privacy regulators
- Associated legal defence costs

The importance of the annual audits should not be overlooked. Once you uncover any unidentified cyber security issues, it becomes possible to proactively address them before cyber criminals can make their move. By having access to periodic cyber security evaluations and the subsequent reports, your businesses' leadership can more accurately assess the underlying business risks, and keep the organization safe from lurking bad actors.

We therefore also recommend having a robust system embedded within your business to review, prioritize, and implement any recommendations or suggestions that result at the completion of these audits. This may involve creating an internal security team or engaging with 3rd party providers specialising in this type of engagement.

Business Benefit: Business As Usual

Timeframe: Jul-22 - Jan-23

Cost/Effort: 1 - 2 Days, $10,000 - $20,000 p/a

Disaster Recovery, Risk and Resiliency - Disaster Recovery Plan

Business Problem

Planning for disruption to the business before it happens means that when an issue occurs the downtime will be shorter, and the business expectations can be met. A disaster recovery or business continuity plan should be in place to ensure that business requirements are meet to an acceptable level when a disruptive event occurs.

Current Situation

needs reviewing

Recommendation

We recommend creating a disaster recovery plan, including documenting the RTO and RPO for each critical IT service and collating an emergency contact list. We recommend talking to each department re requirements and possible manual alternatives that can be used. We also recommend formally testing the IT DR plan.

Business Benefit: Business As Usual

Timeframe: Apr-23 - Oct-23

Cost/Effort: 1 - 2 Weeks, $10,000 - $20,000 one-off

Should Do

Information Assets - Key applications

Business Problem

Out of support, or "version locked" applications or ERPs present a risk in that they are difficult to improve and support. Older versions can also have security vulnerabilities. Upgraded versions, or different applications can provide business advantages, increase staff productivity, add value to the customers, and reduce risk. A good question to ask is what is the oldest piece of technology in the business? How does this limit our business or add risk?

Current Situation

MRP or ERP application could be investigated

Recommendation

We recommend confirming the roadmap for the ERP and supporting applications. Any major change, upgrade or replacement of an ERP system could be a 1-2 year end to end project so it needs to begin early.

A high-level project plan of the steps and timeframes should be completed this year, and resources across the company committed to implement it. An example of the steps required is given below:

1. Confirm how we will deal with ERP modifications

2. Document current modifications and configuration in the ERP

3. Gather and confirm business requirements (include subsidiaries?)

4. Research and confirm list of potential vendors – initial demo.

5. Perform RFP process

a. Confirm how responses will be scored (based on business requirements)

b. Write and send RFP

c. Get responses and presentations

d. Collate and score responses and shortlist vendors (down to 2 or 3)

e. Final solution presentations

6. Collate and score responses and select vendor

7. Kick off project:

a. Development

b. Test/pilot

c. User Acceptance Testing

d. Sign Off

e. Cutover

f. Support

8. Next phase of feature rollouts (optional)

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 2 - 4 Months

Information Assets - Finding and Saving information

Business Problem

Making relevant information easy for staff to find helps improve efficiency and prevent frustration. A recent statistic said that 83% of staff have had to recreate a document which already existed because they were unable to find it. Having a complex folder structure that is filled with unnecessary or irrelevant files can also encourage staff to "Silo" the information they create in places that are not shared with the rest of the company, and may not be backed up or protected. Properly communicating the standards around how staff save information - where to save, how, what file names to use etc. makes information easy for everyone to find.

Current Situation

A lot of data is spread in different locations or difficult to find. Historical knowledge of staff hides this.

Recommendation

We recommend that a standard around saving information is created and communicated with all staff. This standard will affect all users in the business, so some broad steps are shown below:

1. Gather information on what is currently used; the folder structure, the permissions, the age of documents etc.

2. Have workshops/interviews with key staff to confirm their requirements and gather feedback.

3. Confirm the desired "source of the truth" and folder structure for each team and communicate this.

4. Create the new folder structure and copy files to it on a team by team basis, making the old files and folders read-only.

5. Archive all unneeded files.

6. Implement annual archive/clean up of files and folders.

We also recommend investigating moving all company files to a document management solution. This could be a simple solution such as SharePoint via Office 365 which allows features such as versioning, sharing links, co-authoring and metadata, or could be a more feature-rich document management solution such as M-Files, iManage or NetDocuments.

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 1 - 2 Weeks

Information Assets - Drive Encryption

Business Problem

Even a computer that has a password on it can have the data on it accessed by removing the hard drive and installing it in a second computer. There is a risk that if a laptop was stolen sensitive data that is stored on the hard drive could be accessed. Enabling encryption, such as BitLocker or FileVault, prevents access to the data on a computer without the password. Likewise, portable data storage, such as removable USB drives or SD cards, are still widely used. As these are typically small devices the risk of loss is increased and data is readily accessible directly from these devices. It is possible to encrypt portable devices to ensure access is only granted after the password is confirmed.

Current Situation

Bitlocker not enabled on laptops or USB drives.

Recommendation

We recommend enforcing full disk encryption on all computers using BitLocker (Windows) or FileVault (Mac). This should be deployed to all laptops first, and then to all computers.

We also recommend an audit of portable storage drives is performed and if portable drives are still required, encryption should be enforced. "BitLocker To Go" can be used to encrypt portable data for Windows devices. There are some requirements for the devices which read the data; we recommend you investigate the continued use of portable data store and the safety which encryption can provide to these devices.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 3 - 5 Days

Cyber Security - User Account Audit

Business Problem

Over time all systems move away from the norm. Temporary access is granted and never revoked. Staff leave and accounts are held open. Regular audits clean up the system and return it to the norm.

Current Situation

Not performed recently

Recommendation

We recommend regular checks are made to remove old staff accounts - at least six monthly. We also recommend that a formal process is created and followed by HR/Payroll/IT for when a user leaves the company - SharePoint can be used to assist with this.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 6 - 8 Hours

Cyber Security - Staff cyber security awareness

Business Problem

Despite the best technology defenses, security issues can still occur if staff are unaware of the risks, and tips to mitigate them. Regular training of staff on good security practices and updating them on the latest security threats can help mitigate the risk of security issues impacting your business.

Regular training your staff via a face to face presentation, and/or via newsletters or posters and including processes in your induction process can be invaluable to help prevent security threats and reduce the risk of financial loss.

Current Situation

No formal training

Recommendation

It is recommended to engage in a staff awareness program aimed at passing on and reminding of this valuable information. Bi-annual or quarterly updates will keep staff aware of changes and new methods of security risks being used.

We also recommend this is included as part of the staff induction process - this is especially important for financial staff.

We also recommend investigating phishing test email software to confirm the improvement in skills.

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 1 - 2 Days, $500 - $750 p/m

Cyber Security - Financial transaction security

Business Problem

"Spear phishing" uses spoofed emails purporting to be from the CEO to convince a finance person to transfer money to an unintended recipient. They often know a lot about your company, and can be very convincing. As they are plain text, they cannot be blocked by technology.

Current Situation

No formal training

Recommendation

We recommend enforcing a policy within the Finance team so that all large financial transactions require a face to face or phone verification from the staff member requesting. Staff should be made aware of the risks of relying on electronic communication.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 1 - 2 Days, $100 - $150 p/m

Governance, Policy and Process - IT Policies

Business Problem

IT policies are important to inform the users of the company’s position and set expectations on what is permitted and what is not. It should be easy to read, up to date and available in a location available to all staff. Common problems we see in IT Policy documents is that they do not cover mobile devices or tablets, they do not cover saving company data on personal devices or cloud services, they do not cover BYOD devices, they do not cover social media sites, they do not cover working in public locations.

Current Situation

IT policy could be updated

Recommendation

We recommend that the current IT Policy is reworded to use less formal language; it should be readable and understandable by all staff and set expectations on how they should safely use technology.

We recommend that the policy is clearer on the expectations of sharing sensitive company data with external parties or copying it onto unmanaged devices (such as USB drives) or cloud services (such as DropBox).

We recommend some guidance for social media is given.

We recommend that the IT policies (and all company policies) are easily accessible by all staff via a web based Intranet such as SharePoint.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 2 - 3 Days

Information Assets - Business Process Efficiency

Business Problem

It is important that the systems and processes in a business allow "repeatable execution" ensuring that the processes you do regularly are done in a efficient, consistent manner. Common problems are bottlenecks around single staff members, duplication of effort (e.g. entering the same data in multiple systems), and ensuring that the data being inputted is useful at the end of a process when it is reported on. Another common problem is the use of paper forms - electronic forms and workflows are smarter, location agnostic and can provide alerts and reminders to ensure the process doesn't stall.

Current Situation

Business process have not been reviewed recently

Recommendation

We recommend that all business processes are mapped and documented initially. Then solutions to any duplication, bottlenecks or pain points can be investigated using technology where appropriate.

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 1 - 2 Weeks

Productivity and Business Advantage - Company communication

Business Problem

Historically many companies use email to communicate and share information. This has resulted in many staff being inundated with large amounts of email that they struggle to keep up with. Often the email is irrelevant or unimportant and ends up as clutter. There are better tools available to allow more timely communication and collaboration and reduce email clutter - like SharePoint or Basecamp intranets, team collaboration apps like Teams or Slack, simple task management apps like Planner or Trello. Many of these tools are included in Office 365 plans or have free versions.

Current Situation

Teams barely used and not used well

Recommendation

We recommend investigating more modern apps to help with communication and collaboration in the business. We recommend a demonstration of some of the tools with key staff to let them better understand the possibilities.

The following tools could help:

- Microsoft Teams should be trialed with some staff to improve communication and collaboration - perhaps for IT projects first. Teams allows group chat, audio and video calling, and provides a central location for team/project related files and notes.

- SharePoint could be used as a central point of communication in the business. SharePoint is like Lego - out of the box you have all the parts but have to assemble it yourself. Again a demo can help you understand what it can do. For example, it could be used for company news, events, announcements, a health and safety site, hosting company policies and procedures, provide companywide standard forms such as leave forms or expense forms with automated workflows to remove need for paper or manual processes.

- Planner can be investigated to allow simple task management for projects underway.

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 1 - 2 Days

Could Do

Information Assets - Computer hardware rotation

Business Problem

A rotation policy ensures that no machine in the business goes beyond its use by date, which prevents unnecessary disruption and inconvenience to the users. It also prevents the unexpected expense of replacing a machine that fails or is unusable due to age.

Current Situation

No formal rotation in place - "noisiest"" staff get newest computers

Recommendation

We recommend that a hardware rotation policy is implemented and the client computers are proactively replaced every 5 years at least. Depending on the purchasing method it can be advantageous to stagger the purchase of new devices over time rather than have one large hit of costs. This might be irrelevant if devices are leased.

Business Benefit: Added Value

Timeframe: Jan-23 - Jul-23

Cost/Effort: 2 - 3 Days, $40,000 - $50,000 p/a

Information Assets - Emerging technology

Business Problem

Emerging technologies should be investigated to see if they could provide benefit or a competitive advantage to the business or customers, or if they could disrupt the industry as a whole. Emerging technologies include Internet of Things (IoT), speech recognition, robotics, artificial intelligence (AI), drones, 3D printers, virtual reality (VR), augmented reality (AR), RFID.

Current Situation

Could look at 3D printers in developing new products

Recommendation

We recommend that the IT team spend some time researching and work-shopping any new technologies that could disrupt your industry - for example Internet of Things (IoT), speech recognition, robotics, artificial intelligence (AI), drones, 3D printers, virtual reality (VR), augmented reality (AR), RFID.

Any relevant technologies should be further investigated and added to the IT roadmap.

Business Benefit: Bleeding Edge

Timeframe: Jul-23 - Jul-24

Cost/Effort: 1 - 2 Days

Productivity and Business Advantage - Effective Remote Working

Business Problem

The shift to remote working is a different experience for each person and organization. While some teams and organizations have thrived, most have found challenges with staff engagement, collaboration and accountability due to the lack of in-person interactions around the office. With remote working, have you noticed reduced engagement and productivity? Is this affecting performance and impacting the health of your team and organization? How do you know the effectiveness of your teams and projects are tracking the same or better? Which online tools or cloud applications do you use to facilitate meetings, presentations or projects?

Current Situation

Many staff unable to work remotely due to nature of manufacturing. Those that do WFH dont have formal comms channels.

Recommendation

We recommend that the business requirement for flexible working is reviewed. Once the requirements are known we recommend looking at what challenges are faced and how technology can assist to solve them.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 4 - 5 Days

Cyber Security - Physical Security Review

Business Problem

As well as applying digital measures to protect your technology and data, it is important to regularly review your physical security measures. This review should include all measures that restrict access to your premises – swipe cards, door and a window locks, cameras, manning of reception areas, after hours measure etc. with a focus on what areas require more security. It should also include reviewing staff awareness of physical security – are they aware of the risk of someone coming in the door behind them, or viewing their laptop screen in a public place? Another important part of this review would be what policies and procedures you have in place for when staff are working from home or remotely, and what policies you have in place around paper information and how this is stored.

Current Situation

Not performed recently

Recommendation

We recommend performing a regular security review at least annually to review all physical security measure in place, including reviewing access to your premises, swipe cards, keys, security cameras, alarms, staff awareness, policies on working from home and policies for handling and securing paper documents. Any recommendations from the review should have tasks in place to resolve or mitigate any issues found.

Business Benefit: Business As Usual

Timeframe: Jan-23 - Jul-23

Cost/Effort: 3 - 4 Days, $3,500 - $5,000 one-off