

I.T. Review & Recommendations

For: Acme

Prepared by: Kinetics Group
Author: John Smart
Date: Dec 04, 2018
Document Reference: IT Review
Version: 1.0

Executive Summary

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

This document outlines the results of work done by John Smart from Kinetics and Joe Bloggs and Marty Bloggs from Acme in Dec 2018 to review the many questions in the IT best practice review.

Acme have a heavy reliance on the BellAX ERP system which is now out of support. Investigating cloud applications to replace this would reduce critical business risk and increase staff productivity.

Acme should investigate cloud applications to provide best in class features.

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

- Improve ERP systems to improve staff efficiency
- Ensure that all necessary regulations are compliant and documented
- Utilise best of breed commodity cloud services to improve business processes

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

1. This executive summary.
2. The I.T. Strategy and Priorities for Acme.
3. Outline of our understanding of the current state of Acme.
4. A summary of the recommendations.
5. Details of the recommendations, broken into 'Must Do', 'Should Do' and 'Could Do'.

I.T. Strategy



People

- Improve ERP systems to improve staff efficiency
- Make information easier to find by staff through archiving of old data
- Perform security awareness training for all staff



Process

- Ensure that all necessary regulations are compliant and documented
- Introduce IT processes to ensure consistency and reduce risk of reliance on one staff member
- Update the company IT policy and distribute to all staff

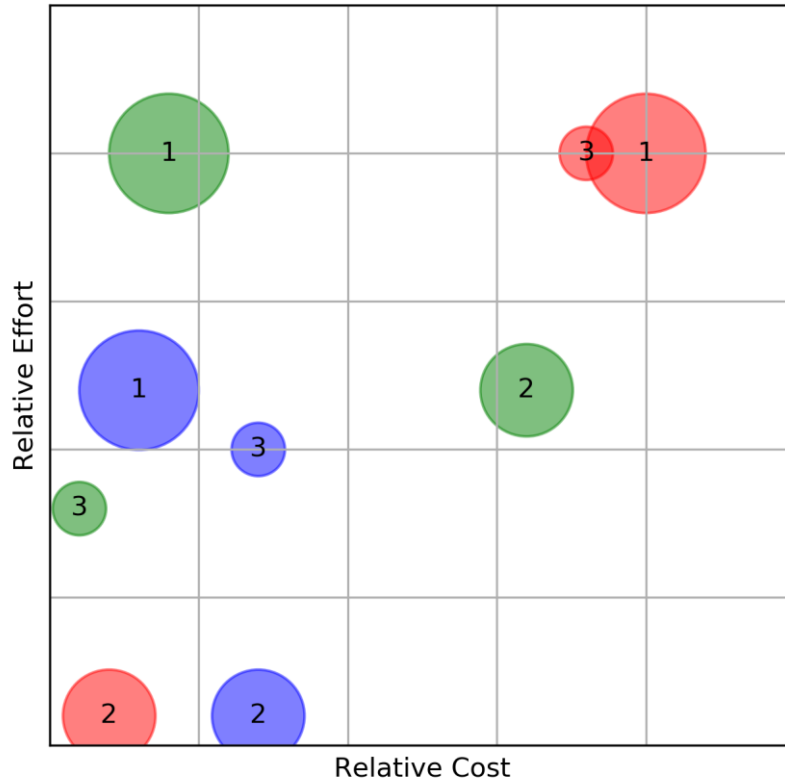


Technology

- Utilise best of breed commodity cloud services to improve business processes
- Use ATP technology to improve security.
- Improve Public Website security as this is the core of the business

Priorities

The following graph plots the most important recommendations by the relative cost, effort and priority. Bubbles that are large (high priority) and are in the bottom left quadrant (low cost and effort) are easily addressed first.



People	Process	Technology
<ol style="list-style-type: none"> 1. Improve ERP systems to improve staff efficiency 2. Make information easier to find by staff through archiving of old data 3. Perform security awareness training for all staff 	<ol style="list-style-type: none"> 1. Ensure that all necessary regulations are compliant and documented 2. Introduce IT processes to ensure consistency and reduce risk of reliance on one staff member 3. Update the company IT policy and distribute to all staff 	<ol style="list-style-type: none"> 1. Utilise best of breed commodity cloud services to improve business processes 2. Use ATP technology to improve security. 3. Improve Public Website security as this is the core of the business

I.T. Roadmap - the next two years

Jan - Jun 2019

- Staff cyber security awareness
- Saving information
- Password Policy
- Police checks
- Cloud usage
- Business Process Efficiency
- Company communication
- Regulatory requirements
- Information asset protection
- Legal Software
- Data Privacy Policy



Jul - Dec 2019

- Saving information
- Key applications
- Mail Archiving
- Improve Public Website security
- IT Policies
- Sharing Technical Knowledge
- Advanced threat protection
- Business Intelligence and Reporting



2020

- Saving data
- Paper-less or Paper-light
- Emerging technology
- PC Encryption
- Software Maintenance Agreements

Current State



Organisation

- Auckland, Melbourne, Sydney
- Approximately 85 staff, with 70 computers.
- 1 IT staff
- There are 1 I.T. staff.



Systems

- Salesforce - SaaS crm
- Connectwise - On-premise management
- Microsoft CRM - On-premise crm
- BellAX - On-premise erp



Issues and Risks

- Keep having power issues
- Slow internet connection



Projects

- Replacing email server
- Replacing server
- Introducing BI reporting

Current State Summary Graph

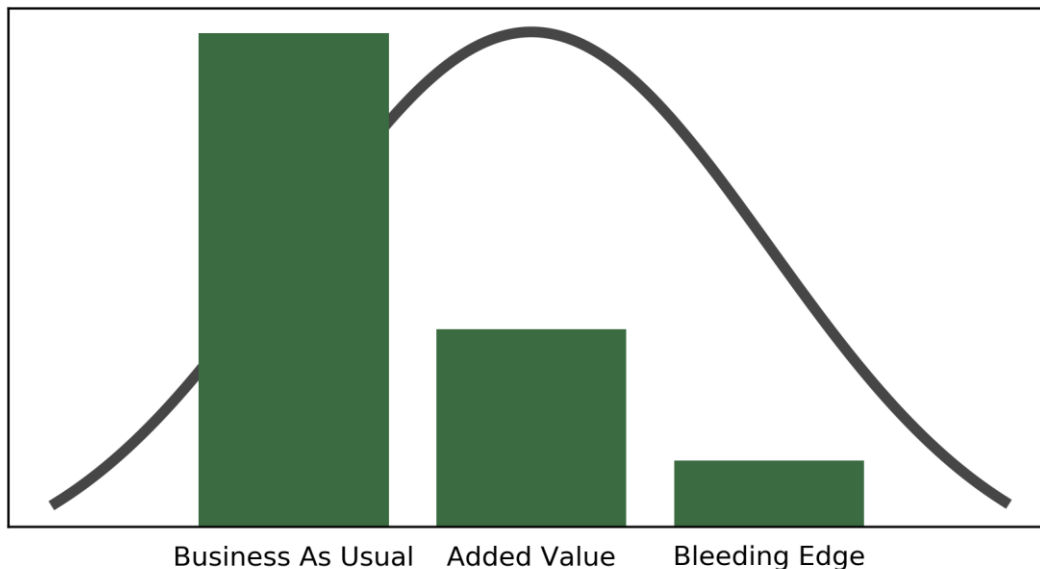
The following outlines the current state of Acme in the various categories measured. The benchmarks shows current average response across all completed reviews.



Recommendation Summary

Business Benefit

The following maps the "business benefit" of each recommendation. Are the recommendations focussed on business as usual, adding value to the staff, or are we pushing the envelope? The bell curve indicates the ideal scenario, with most IT effort going into adding value.



Recommendation Index

The following outlines an index of all recommendations. Note that all costs are approximate, and the approximate effort required to implement is included to give an indication of the work involved/complexity of the task.

Must Do - Action Immediately

Title	Effort	Cost one-off	Cost ongoing
Staff cyber security awareness	8 - 12 Hour(s)	\$1500 - \$2250	\$0 - \$0 per month
Saving information	1 - 2 Week(s)	\$500 - \$1000	\$40 - \$50 per month
Password Policy	2 - 4 Week(s)	\$1000 - \$2000	\$0 - \$0 per month
Police checks	2 - 4 Hour(s)	\$50 - \$300	\$0 - \$0 per month
Cloud usage	1 - 2 Week(s)	\$5000 - \$6000	\$800 - \$1200 per month
Business Process Efficiency	6 - 8 Week(s)	\$5000 - \$10000	\$0 - \$0 per month
Company communication	1 - 2 Week(s)	TBC	TBC
Regulatory requirements	7 - 14 Day(s)	\$5000 - \$10000	\$0 - \$0 per month
Information asset protection	1 - 2 Month(s)	\$1000 - \$2000	\$100 - \$200 per month

Should Do - Plan for Action

Title	Effort	Cost one-off	Cost ongoing
Legal Software	1 - 1 Hour(s)	TBC	TBC
Data Privacy Policy	5 - 6 Day(s)	\$3000 - \$5000	\$400 - \$500 per annum
Key applications	4 - 6 Month(s)	\$50000 - \$66000	\$500 - \$700 per month
Mail Archiving	10 - 20 Hour(s)	\$0 - \$0	\$50 - \$100 per month
Improve Public Website security	5 - 7 Day(s)	\$0 - \$0	\$200 - \$300 per annum
IT Policies	3 - 4 Day(s)	\$4000 - \$5000	\$0 - \$0 per month
Sharing Technical Knowledge	1 - 2 Week(s)	\$0 - \$0	\$3000 - \$4000 per month
Advanced threat protection	1 - 2 Week(s)	\$5000 - \$7000	\$100 - \$200 per month
Business Intelligence and Reporting	1 - 2 Week(s)	\$3000 - \$5000	\$120 - \$150 per month

Could Do - Investigate

Title	Effort	Cost one-off	Cost ongoing
Saving data	1 - 2 Week(s)	\$3000 - \$5000	\$0 - \$0 per month
Paper-less or Paper-light	1 - 2 Day(s)	\$2000 - \$3000	\$0 - \$0 per month
Emerging technology	1 - 2 Day(s)	\$5000 - \$10000	\$0 - \$0 per month
PC Encryption	1 - 2 Hour(s)	TBC	TBC
Software Maintenance Agreements	1 - 2 Day(s)	\$3000 - \$4000	\$0 - \$0 per month

Recommendations

Must Do - Action Immediately

Information Assets - Staff cyber security awareness

Business Problem

Despite the best technology defences, infections can still occur if staff are unaware of the risks. Regularly training of staff on good security practices, and updating them on the latest security threats can help mitigate the risk of security risks impacting your business. We have done this training for other clients via short presentations, or via internal email newsletters.

Current Situation

No formal staff cyber awareness training is currently performed.

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.

Effort	Time frame	Cost one-off	Cost ongoing
8 - 12 Hour(s)	Jan 2019 - Jan 2019	\$1500 - \$2250	\$0 - \$0 per month

Information Assets - Saving information

Business Problem

Files that are saved to workstations create issues with data loss & data duplication. This means that there can be several versions of the same file floating around the environment or could lead to data loss if a workstation were to crash.

Current Situation

Suspect files are stored in users Dropbox

Recommendation

We recommend investigating moving all company files to a document management solution. This could be 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 or iManage.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Mar 2019 - Sep 2019	\$500 - \$1000	\$40 - \$50 per month

Cyber Security - Password Policy

Business Problem

Passwords are still the primary technique to control computer security. We can set minimum length, maximum age, complexity and lockout policies. The current thinking is that minimum length is the most important - longer is stronger! Make the passwords as long as possible - 12 characters or more. Get people to use phrases instead of words/numbers.

Current Situation

Passwords are weak - only 6 characters, no complexity enabled and no account lockout.

Recommendation

We recommend enabling account lockout immediately – there should be no side effects from this.

We also recommend enabling password complexity and changing the minimum password length to 12 characters to enforce stronger passwords. This will require good communication to the staff warning them of the change and we recommend it is implemented in batches of users to reduce the impact on IT support.

Effort	Time frame	Cost one-off	Cost ongoing
2 - 4 Week(s)	Jan 2019 - Jan 2019	\$1000 - \$2000	\$0 - \$0 per month

Cyber Security - Police checks

Business Problem

Police checks will identify any criminal or fraudulent activity of a potential staff member before they are employed. Although not an IT question, this has come up in the context of these reviews.

Current Situation

Police checks not currently performed on new staff.

Recommendation

It is recommended that the recruitment process be reviewed to confirm if this is being checked.

Effort	Time frame	Cost one-off	Cost ongoing
2 - 4 Hour(s)	Jan 2019 - Jun 2019	\$50 - \$300	\$0 - \$0 per month

DR and Resiliency - Cloud usage

Business Problem

There are a number of cloud services that can provide benefits to companies - software as a service such as Office 365, infrastructure as a service such as Azure, local datacentres, or a combination of all. Before any major IT project all cloud scenarios should be investigated to see if they can add value to the business.

Current Situation

All ERP systems are hosted on on-premise server infrastructure.

Recommendation

We recommend moving on-premise servers to Azure Infrastructure as a Service. This moves all hardware costs to an op-ex, pay as you go expense and also provides a number of benefits around security, resiliency and reliability.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Jan 2019 - Jun 2019	\$5000 - \$6000	\$800 - \$1200 per month

Staff Capability - 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.

We think this is really important.

Current Situation

Business process hasnt 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.

Effort	Time frame	Cost one-off	Cost ongoing
6 - 8 Week(s)	Jan 2019 - Jan 2019	\$5000 - \$10000	\$0 - \$0 per month

Staff Capability - 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. Often these tools can be shared with external parties, such as partner, customers or suppliers to again improve communication with these parties.

Current Situation

Communication is not great

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 company-wide 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.

Effort	Time frame
1 - 2 Week(s)	Mar 2019 - Jun 2019

Regulatory - 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

Acme needs to be PCI compliant as they store credit card information.

Recommendation

Follow the steps to ensure there is PCI compliance.

Effort	Time frame	Cost one-off	Cost ongoing
7 - 14 Day(s)	Jan 2019 - Jun 2019	\$5000 - \$10000	\$0 - \$0 per month

Regulatory - 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?

Current Situation

We dont know where staff are saving information.

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 using secure cloud services instead of email or using Information Rights Management from Office 365 may be able to help.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Month(s)	Jan 2019 - Jun 2019	\$1000 - \$2000	\$100 - \$200 per month

Should Do - Plan for Action

Information Assets - Legal Software

Business Problem

To ensure software licensing is compliant and you are meeting your legal obligations. Microsoft and other software companies do perform random licensing audits of their software. xddfsdf

Current Situation

Not confident that all software is legal. Needs checking.

Recommendation

We recommend performing an audit of the software licenses in use and compare that to the software licenses purchased. The shortfall (if any) should then be addressed as a matter of priority.

Effort	Time frame
1 - 1 Hour(s)	Jan 2019 - Jan 2019

Information Assets - Data Privacy Policy

Business Problem

Data privacy became a hot topic in 2018. This was driven by three main factors:

1. The GDPR (General Data Protection Regulation) which came into effect in Europe in May 2018. This introduced strict regulations on what private information is, how to get consent from users, how to deal with breaches, and when personal information must be deleted. The fines for not complying were large; €20 million or up to 4% of the annual worldwide turnover. Although European regulation, it applies to any company that stores personal information for EU citizens so potentially impacts all companies world-wide.

2. Updates to the Australian Privacy Act which makes data breach notification compulsory as of February 2018. This means that if an individual's personal information is leaked and likely to result in serious harm the company is required by law to notify the individual(s). Again, the fines for not complying were increased to up to \$2 million.

Updated privacy regulations aim primarily to give control to citizens of their personal data. It means that citizens are better aware of how their personal data will be stored, used and shared.

Current Situation

No data privacy policy in place

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?

Effort	Time frame	Cost one-off	Cost ongoing
5 - 6 Day(s)	Feb 2019 - Jun 2019	\$3000 - \$5000	\$400 - \$500 per annum

Information Assets - Key applications

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.

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

The ERP system is out of date, version locked and unable to be supported. It will not provide an eCommerce website which is required.

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.

Effort	Time frame	Cost one-off	Cost ongoing
4 - 6 Month(s)	Jul 2019 - Dec 2019	\$50000 - \$66000	\$500 - \$700 per month

Information Assets - Mail Archiving

Business Problem

Archiving can be done for two reasons; 1. to reduce space and reduce clutter (less chance of problems, and make current mail easier to find), 2. to maintain compliance by ensuring critical data is retained for a certain length of time (e.g. retaining copy of all email sent in and out).

Current Situation

No mail archiving, management have very large mailboxes

Recommendation

We recommend implementing the email archiving features:

1. We recommend enabling "Personal Archive" for all staff. This creates a second "archive" mailbox for each staff member and automatically moves email to it after a certain age - 2 years by default. This helps reduce the size of the "live" mailbox which helps reduce issues caused by large mailboxes.
2. We recommend enabling "Legal Hold" features on Office 365 to retain a copy all email regardless of whether the staff delete it.

Effort	Time frame	Cost one-off	Cost ongoing
10 - 20 Hour(s)	Jul 2019 - Dec 2019	\$0 - \$0	\$50 - \$100 per month

Cyber Security - Improve Public Website security

Business Problem

Having your public website defaced or brought down can lead to a loss of reputation. Popular website systems such as "WordPress" or "Joomla" are often targeted by hackers so need to have regular security patches applied. Because public websites are often developed by third parties (and not the IT team or IT provider), the security of websites can get missed.

Often public websites and the information on them, are hosted externally and managed by a third party. If the third party ceases to exist, or data gets corrupted or deleted, you could potentially lose all the information on your public website.

It is becoming more common to have your public facing website running on securely on HTTPS to prove that your site is who it says it is. This will also increase your ranking in Google's search engine. Large internet companies such as Google and Microsoft are pushing all websites to be HTTPS to prevent the risk of malware and cryptolocker.

Current Situation

Not sure - website was created by Marketing team, no IT involvement

Not sure if it is backed up - not monitored or controlled by IT team.

Public website not currently HTTPS.

Recommendation

We recommend that the current website provider ensures that the website CMS is regularly updated. We also recommend that the website is presented on HTTPS if possible - again the website provider can assist with this. This should be done for all public websites owned by the organisation.

We recommend that we implement regular backups of your public websites. Include should be included in your Disaster Recovery (DR) plan and include a periodic test restore.

We recommend that the website is presented on HTTPS if possible - the website provider can assist with this. This should be done for all public websites owned by the organisation.

Effort	Time frame	Cost one-off	Cost ongoing
5 - 7 Day(s)	Jul 2019 - Dec 2019	\$0 - \$0	\$200 - \$300 per annum

Governance and Management - 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

The current company IT Policy has not been updated since 2003.

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.

Effort	Time frame	Cost one-off	Cost ongoing
3 - 4 Day(s)	Jul 2019 - Dec 2019	\$4000 - \$5000	\$0 - \$0 per month

Governance and Management - Sharing Technical Knowledge

Business Problem

Documenting and sharing technical configuration information is critical to reduce the risk of vital knowledge being kept in one person's head. Documentation speeds up issue resolution and reduces

support costs. Where is it stored? Who has access to it? Is that appropriate? Does it contain confidential information such as passwords?

Current Situation

All technical information known by internal IT staff member but not documented or shared.

Recommendation

We recommend all IT systems are documented. This documentation should be readily available to IT staff but locked down from standard user availability. This documentation should also be readily available in the event of a server failure or disaster. This documentation would include:

- Overview of configurations, diagrams and "why" systems exist.
- Usernames and passwords for all equipment
- IP addresses for all equipment
- Physical and virtual server roles and configurations
- Backup configurations and procedures
- Network and server diagrams
- Networking configurations (wireless, firewall, switching, VLAN)
- Public internet, public certificate, public DNS and website information
- Overviews, summaries and key decisions
- Contact details for third parties
- License keys and information
- Application configuration information
- User and Computer set up procedures

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Jul 2019 - Dec 2019	\$0 - \$0	\$3000 - \$4000 per month

DR and Resiliency - Advanced threat protection

Business Problem

Firewalls protect your business from the outside world. Traditional firewalls only block certain traffic from coming in from the outside world. However, modern "next gen" firewalls provide advanced threat protection where they check the link or file you are opening against a known list of "bad" links and block it. This is another tool in the tool belt to prevent ransomware or cryptolocker attacks.

Current Situation

No ATP in place on firewall, no DNS filtering or AV ATP in place.

No PC encryption currently in place

Recommendation

It is highly recommended that additional security features be investigated to reduce the current risks. A firewall capable of Advanced Threat Protection and Web Blocking is recommended.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Jul 2019 - Dec 2019	\$5000 - \$7000	\$100 - \$200 per month

Staff Capability - 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 behaviour
- To improve visibility of trends
- To turn data into actionable information
- To improve efficiency

Current Situation

No BI in place currently

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.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Jul 2019 - Dec 2019	\$3000 - \$5000	\$120 - \$150 per month

Could Do - Investigate

Information Assets - Saving data

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?

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.

Current Situation

We dont know where staff are saving information. The company needs a proper ERP

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 using secure cloud services instead of email or using Information Rights Management from Office 365 may be able to help.

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
6. Collate and score responses and select vendor
7. Kick off project
8. Next phase of feature rollouts (optional)

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Week(s)	Jan 2020 - Dec 2020	\$3000 - \$5000	\$0 - \$0 per month

Information Assets - Paper-less or Paper-light

Business Problem

Creating electronic forms and changing signing or authorising processes to electronic can speed up processes, ensure things are not lost and get around issues relating to geography. Accounts payable processes can especially benefit from this technology.

Current Situation

Many paper processes in use currently.

Recommendation

We recommend that initially one process that uses paper forms is replaced with an electronic such as SharePoint, PowerApps, or Abode Signing. Once this is implemented and bedded in, other processes should be identified and replaced in a similar manner.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Day(s)	Jan 2020 - Dec 2020	\$2000 - \$3000	\$0 - \$0 per month

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 into 3D printing to assist with the prototyping process

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.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Day(s)	Feb 2020 - Dec 2020	\$5000 - \$10000	\$0 - \$0 per month

Cyber Security - PC 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, prevents access to the data on a computer without the password.

Current Situation

No PC encryption currently in place

Recommendation

We recommend enforcing full disk encryption on all laptops initially.

Effort	Time frame
1 - 2 Hour(s)	Jan 2020 - Dec 2020

Governance and Management - Software Maintenance Agreements

Business Problem

To ensure software licensing is compliant and you are meeting your legal obligations. Microsoft and other software companies do perform random licensing audits of their software.

It is important to ensure support and updates of key applications are available when needed. If we have a problem with your key application, will we be able to call them up and get support? Will we get upgrades for free (which might be needed to support a new version of Windows for example)?

Current Situation

All software is not under a current maintenance agreement

Recommendation

We recommend performing an audit of the software in use and ensure that viable support is available for all software. For any software that is not under support plans should be made to replace or upgrade it.

Effort	Time frame	Cost one-off	Cost ongoing
1 - 2 Day(s)	Jan 2020 - Dec 2020	\$3000 - \$4000	\$0 - \$0 per month