Amstelveen

Risk Update

Edition 2, December 2019

Contents

Preface

Welcome to the second edition of our Risk periodical, the 'Risk Update'. In this edition we have delved into two specific areas of technology risk and covered some of the cultural aspects of good Risk Management.

Cybersecurity related risks continue to be of high interest to Boards, Audit Committees, and Risk and Technology functions. Data from the Office of the Australian Information Commissioner indicates that individuals remain the most readily compromised component of a technology environment. **Ed Little** has provided a breakdown of good practices for protecting online user accounts. This is the first in a forthcoming series of articles which explain techniques for keeping your data safe online.

At an organisational level, technology functions are increasing their use of data processing automation. **Zachary Chapman** has considered how they can manage the associated risks by using Workflow Automation tools. These have the potential to improve data integrity while simplifying operational processes.

Finally, Risk Culture has continued to be of interest to regulators and the media. We explain how organisations usually measure and assess their risk culture, and some ways to encourage positive risk behaviours.

I hope that you find this publication both useful and interesting. To provide feedback or input on content, feel free to contact info@amstelveen.com.au.

David van Gogh
Director

Practical Tips for Staying Secure in a Connected World

Part One: Managing your digital identity

Ed Little

This is the first article in a series looking at personal security, practical tips for staying safe online and managing your digital identity. In this series we will cover how to protect your accounts online (the subject of this article), avoiding scams and safeguarding your devices and data.

Why We Need to Act

The last few years have seen some incredible data and privacy breaches. Facebook's woes come readily to mind with repeated appearances before the US courts following the controversy in the 2016 US election and the Cambridge Analytica breach, but they aren't the only ones in the spotlight.

Last year Marriott International lost 500 million accounts, Under Armour 150 million and Equifax 143 million. Unfortunately, 2019 has not fared much better. 540 million Facebook accounts were lost by companies with poor security practices who used Facebook to authorise their users. Canva, the online graphics platform reported a breach of over 140 million accounts following a hack on their systems in May.

It may seem like the rate of breaches is increasing, certainly this is part of the story. The observed increase can also be attributed to the increasing adoption of mandatory data breach reporting legislation by governments across the world. The USA, EU, Canada and Australia all have mandatory data breach reporting laws that cover intentional (e.g. attackers stealing data from a database) and unintentional (e.g. mistakenly giving personal information to the wrong person) data loss. So then, it's not simply that more breaches occur, it's also because we are being made aware of breaches that may have otherwise gone unnoticed.

According to the Office of the Australian Information Commissioner (OAIC), there were over 950 notifiable breaches between July 2018 – June 2019 , averaging almost 80 breaches per month. In most cases, contact information was stolen, but financial, health and Tax File Numbers were also lost in breaches. Reading the statistics, it might feel like the only options are to remove yourself from the internet and delete all your accounts in attempt to protect your personal information or resign yourself to the 'fact' that losing your data is the cost of entry in the connected world. Whether you're a digital native or someone who doesn't consider themselves particularly 'tech-savvy' and finds it all a bit overwhelming, the tips and suggestions in this series will provide you with some pragmatic options to help you stay safe online and improve the way you manage your digital identity.

Protecting Your Accounts and Privacy

Two-Factor Authentication (2FA)

One of the best ways to secure your account is to add an additional step or 'factor' when logging into your accounts. The most common version of this is to use a 'token' to generate a six or eight digit code that you use after logging in with your username and password. These token generators could be a physical tag, provided by your bank or employer, or a 'soft token'.

In the last few years, the rising popularity and convenience of digital or 'soft tokens' which make use of an app on your smartphone, has made them the ideal way to manage 2FA for personal accounts. Password managers and apps like the Google or Microsoft Authenticator make managing multiple tokens easy and remove the need to carry multiple physical token generators on keyrings or in backpacks. They have the added benefits of being less likely to be lost (assuming of course that you aren't prone to losing your phone) and are often protected by biometric security you use to unlock your phone.

Digital tokens are quite easy to set up, in most cases by scanning a QR Code using your phone's camera and entering the code generated by the app is all that's required to get setup. Most services offering 2FA also provide instruction on how to set up 2FA using popular apps like Google or Microsoft Authenticator.

One note of warning regarding 2FA. Many services now offer account confirmation and 2FA by sending a text message to your phone, and while it can be a convenient way to get a token code, it is vulnerable to an attack called sim jacking where an attacker clones your sim card to receive text messages sent to your number. Attackers use this method in combination with stolen credentials to steal the 2FA code from a text message and log in. We would recommend using a digital or soft token like those mentioned above in conjunction with a password manager rather than text message confirmations to protect your accounts.

Password Managers

Most of us have a few 'go-to' passwords we use to manage our online lives and if we're particularly creative, maybe even a separate password for work. Often, these passwords are based on information that makes them easy to remember, anniversaries, the names of loved ones or a favourite sports team. The downside to this approach is twofold.

Firstly, if we had a fairly benign conversation about your family, your interests or what you got up to on the weekend I'd have a fairly good list of things to try. To make matters worse, these days it isn't necessary to have the conversation, Facebook, Instagram, LinkedIn and Twitter are all far easier and faster places to get that information and you won't even know I'm poking around.

Secondly, remembering passwords is painful at the best of times, which is why we tend to make them memorable. It's also why we tend to reuse them over and over. Even if you have five or six passwords of varying complexity for social media, e-commerce, online banking or work, the stark reality is that even having 10 or 15 passwords is insufficient for safely navigating the modern internet. But who has the brainpower to remember all those passwords?

The best place to start is a password manager. Password managers provide a simple and convenient way to manage your passwords online and offline, working on the principle that it's easier to remember a single complex password than hundreds of passwords for every site and account you have. Password managers have the added benefits of encrypting your data, are available on all your devices and are more difficult to break into than the notebook you keep in the top drawer of your desk.

This all sounds good, but how do password managers actually work and how do you try one? Most modern browsers provide basic password manager functionality, suggesting complex random passwords and automatically filling them in when returning to log into the site.

Chrome, Firefox and Safari all provide these features and provide a syncing service to keep the browsers on your devices up to date with your current passwords. Safari on iOS goes a step further, allowing these passwords to be accessed when signing into your mobile apps. Although not always enabled by default, Google offers a similar service with Chrome and Android.

Top 10 list of most common passwords from the UK National Cyber Security Centre (NCSC) survey, which analysed passwords belonging to accounts worldwide that had been breached.

1.	123456	6.	12345678
2.	123456789	7.	Abc123
3.	qwerty	8.	1234567
4.	password	9.	Password1
5.	111111	10.	12345

Taking things up a notch, there are stand-alone password managers that provide a device-independent way of managing passwords and usually include 2FA soft token integration. These services are excellent if you work across multiple platforms, devices or browsers or if you need a way to securely share passwords in your organisation for shared services or administrative accounts. These services typically integrate with your browser via an extension and can automatically fill in your account details when you log into a site. They may be cloud hosted or available as an app for your device.

There are several options around to choose from that range from free to a few dollars a month, the main difference being the level of customer support available, user experience and extended features like integrating with services like haveibeenpwned.com to actively check and advise you if your accounts have been exposed in a data breach.

Finding a service that's right for you will depend on your budget and how comfortable you are managing and configuring the service. The free services are often open-source projects and require some fiddling to get started, while premium services like 1Password, LastPass or Dashlane are easy to use and provide customer support but come with a premium price tag.

Monitoring for Compromise

Services like haveibeenpwned.com and Google's new Password Checkup Extension provide a service that can help you stay informed about the safety of your accounts by notifying you of suspected breaches. Sometimes having the information and taking steps to secure your account is the difference between losing your account and saving it.

This was illustrated recently with the release of the Disney+ streaming service, which attracted attention in its first week for gaining 10 million new signups far eclipsing the launches of Netflix, Hulu and others. Disney+ also made headlines in its first week for an alleged 'hack' and accounts being sold on the dark web for as low as $3. Bad press aside, the reality is that these account thefts weren't caused because Disney leaked the information, but rather that customers of the service reused passwords that had been leaked previously from other sites allowing attackers to commandeer the accounts and sell them.

Closing Thoughts

Staying safe online is more than just being organised. To a large extent it is a mindset and a willingness to take proactive steps. Thankfully the last few years have yielded several great tools that can help keep us safe without compromising on convenience too much.

In the next article, we will be covering techniques to avoid scams and targeted phishing attacks, and we'll look at steps you can take to protect your devices. The whole series will be published on our website as each article is released.

Data Processing

Maintaining data integrity within an ever changing technology landscape

Zachary Chapman

Technology functions are increasing their use of data processing automation. This article considers how the associated risks of using Workflow Automation tools can be managed.

Introduction

Technology functions are increasing their use of automation for data processing. Automated data processing requires strong systems and supporting infrastructure in order to be leveraged effectively in keeping up with technology transformation.

Companies must ensure processes are being continually streamlined, and avoid the risk of falling behind their competitors due to reliance on legacy systems preventing complete automation integration into business operations.

Automation through Scripting

Traditionally, scripting has been used to automate processes using pre-built commands to run a list of tasks. Scripts, however, require manual initiation, and the list of commands included in the script cannot be deviated from, restricting customisation and the potential for large scale automation.

Job Scheduler Automation

The limitations in the design of scripts can be overcome through the use of a job scheduler, where sequences of scripts are automatically run on a schedule. Job schedulers enable configuration of jobs to run at specific times or when an event is triggered, which can be set up to run in batches after hours to avoid using processing capacity of users during business hours.

Examples of job schedulers include Windows Task Scheduler and the CRON utility for Unix, which come pre-installed on systems supporting the associated operating system. More advanced software such as the Advanced Task Scheduler designed for IBM systems, allows for additional customisation capability for task automation.

Drawbacks of Job Scheduling Systems

Job Schedulers provide powerful process automation that increases productivity in business operations, however there are limitations to the effectiveness of automation between systems, preventing complete integration across platforms in a workflow. Examples are listed below.

- **Siloed job schedulers** that are incompatible with other platforms prevent complete synchronisation of end to end process automation, often requiring manual intervention between processes in a workflow.
- **Processing errors** between platforms are likely to occur due to the lack of a centralised workflow management tool. The risk of human error with the reliance on manual identification and remediation of issues.
- **Security vulnerabilities** on legacy job schedulers reaching end of life that are exempt from patches, provide hackers opportunity to perform malicious activity.
- **Compliance gaps** are likely to emerge in the ability for job schedulers to meet the changing criteria for systems to be considered compliant to the appropriate regulations.

Use of Enterprise Workload Automation

Workload automation tools provide a solution to the limitations of job scheduling systems, by enabling integration of job processing across all platforms supporting business functions. Automated workflows have the following benefits:

Visibility is achieved over the end to end automated process, ensuring issues are highlighted in a centralised system, such as the dashboards used in Control-M, to highlight the success and failures of job completion, with tasks not meeting SLAs being flagged.

Remediation of jobs with issues identified is improved, with manual identification and remediation of issues not required as a result of implementing a centralised monitoring interface to identify areas of concern in real time.

Maintenance of workflow tasks is simplified, in that jobs can be modified in a single, centralised tool, removing the complexity and potential for error that would otherwise be required to update several job schedulers.

Auditing and regulatory compliance is improved with tools such as AutoSys Workload Automation allowing role-based access control for accessing job schedulers, with tracking of changes made to the workflows and reporting available for review and identification of areas of improvement.

User education on the operation of the workload automation tool is simplified, with users supporting the system only requiring education on a single tool. This eliminates the need for companies to employ subject matter experts across a multitude of systems on separate platforms, and saves time and cost associated with the reissuance of education to each.

The unfortunate downside to workload automation is that well established organisations have business processes integrated into existing infrastructure that is outdated.

Organisations should weigh up the costs, risks and benefits associated with a large scale uplift to the current automation tools, and if a parallel or phased implementation of an improved workload automation tool is best suited in integrating current systems to the new automation tool upon refreshment or replacement after reaching end of life.

The Future of Workload Automation

Workload automation tools have provided a necessary uplift to existing automation processing systems, leveraging technologies such as artificial intelligence to provide advanced methods of automation into business environments.

Workload Automation Simplification is emerging with the use of user friendly interfaces removing the requirement for job scheduler experts. Applications, such as Microsoft Flow, allow for pre-built templates

or customised processes to automate workflows on local and cloud based applications. Users must ensure compliance is maintained to security policies, even with a simplified interface.

Adaptation to Emerging Technology is vital to maintain the pace within the ever-changing technological landscape. Systems, such as IBM's Workload Automation Tool, enable automation capability across Internet of Things devices over hybrid cloud environments, and integration of Big Data analytics through Hadoop into the existing infrastructure. Risk management must evolve to accommodate this transformation, ensuring controls are continually updated to ensure sufficient protection is in place for emerging trends.

Machine Learning is being adapted to further automate error detection, correction and prevention. Continuous learning enables mitigation of operational risk of workload automation through trend analysis of systemic issues and identification of trends, removing reliance on human intervention.

Robotic Process Automation allows for "Robot" accounts to be configured and trained by humans and, through machine learning, carry out repetitive tasks and interact with interface objects, such as buttons and fields. Operational risk is prevalent if Robot accounts are configured incorrectly, and account privileges should be managed through tools such as CyberArk's check-in/check-out authentication through encrypted sessions. Failure to do so opens up the risks of using Robot account privileges and access to perform malicious activity.

Closing Thoughts

Workload automation must remain adaptive to the rapidly transforming digital landscape in order to remain effective. Integrity must be maintained, and controls around error detection, user access and logging must be adapted to the new ways of working. The potential for workload automation is limitless if companies embrace change and are willing to sacrifice the time, effort and costs associated with migration away from legacy systems.

Clarifying Risk Culture

An introduction to factors influencing Risk Culture, approaches to measuring it and methods for uplift

David van Gogh

Introduction

Risk culture refers to the behaviours, attitudes and norms in an organisation that affect how risks are considered in decision making.

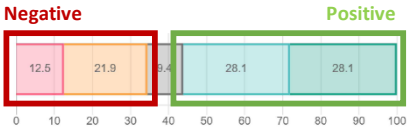
Organisations with a strong risk culture foster transparency and considered decision making. They have long-term performance and incentive structures which make them more resilient, and they encourage staff to 'speak up' when they see potential issues. Conversely, organisations with a poor risk culture encourage short-term decision making which ultimately results in issues, incidents and scandals. For the Boards of APRA regulated entities, having an understanding of the organisation's risk culture is also a regulatory obligation.

This article contains an analysis of factors which influence risk culture in organisations. It also covers typical approaches to measuring and improving risk culture.

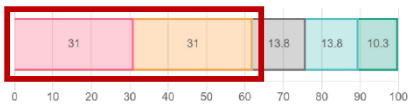
> "…the Board must ensure that… it forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensures the institution takes steps to address those changes"
>
> APRA, Prudential Standard CPS 220 Risk Management, July 2017, s9 'The Role of the Board' (b)

How is Risk Culture Measured?

Risk Culture is measured by identifying behaviours that affect decision making. Usually, this is done by surveying members of an organisation. Respondents are requested to reflect on behaviours that they have observed across a variety of organisational groups (themselves, their teams and their leaders), and responses are aggregated and analysed for areas of relative strength and weakness.



My colleagues take steps to identify risks and prevent issues from occurring



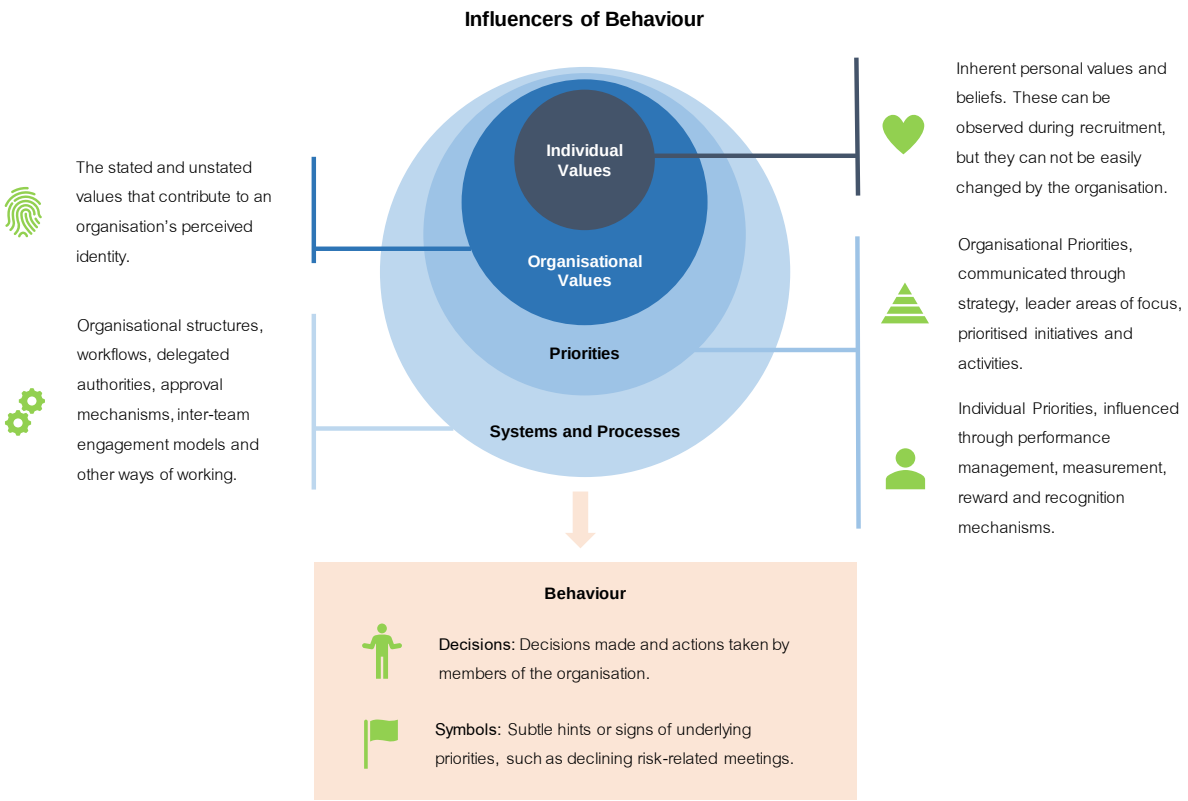
People tend to be recognised for fixing problems rather than preventing them

These assessments allow us to gain a basic understanding of decision making behaviours within an organisation. While survey-based assessments have limitations, they are composed with consideration for removing respondent biases, maximising actionable insights, and allowing for benchmarking across industries or organisation types.

In more complex environments, assessments are supplemented with more in-depth techniques, such as focus groups and deep-dive reviews of organisational structures and processes. These can provide more information on the causes of undesirable behaviour.

What Influences Risk Behaviours?

Behaviours within an organisation are influenced by a complex range of factors. Key factors which influence behaviour are identified in the diagram below.



How can improvements be made?

Changes to culture take time. Improvement activities should focus on enduring influencers on culture; priorities, systems and processes. Such actions often include the following:

- Integrating risk elements into the organisation's strategy;
- Focusing on the importance of risk management in leader messaging;
- Prioritising funding for risk buydown initiatives;
- Strengthening accountability through organisational structures and workflows; and
- Focusing performance management, recognition and reward mechanisms on long-term outputs.

The uplift activities required in the context of a specific organisation will vary. Activities need to be considered against the identified root causes of behavioural issues in specific organisations.

Conclusion

Organisations which focus on Risk Culture make considered decisions, avoid issues and incidents, and are ultimately more resilient. While difficult, Risk Culture can be measured through specifically targeted techniques. These allow for undesirable risk behaviours to be identified, understood and reduced.

Citations

1. Australian Government Office of the Australian Information Commission (27 August 2019). Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019. *Available at: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/*

2. Chrome Web Store. Password Checkup System (2019). *Available at: https://chrome.google.com/webstore/detail/password-checkup-extensio/pncabnpcffmalkkjpajodfhijclecjno?hl=en*

3. Sydney Morning Herald (20 November 2019). 'Thousands of Disney + accounts were hacked and sold online for as little as $4.40'. *Available at: https://www.smh.com.au/business/companies/thousands-of-disney-accounts-were-hacked-and-sold-online-for-as-little-as-4-40-20191120-p53c7l.html*

4. Picheta, R. CNN Business (23 April 2019). 'How hackable is your password?'. *Available at: https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html*

Amstelveen

Amstelveen's team of professionals work on major technology and business change projects, and enhance capability in risk management, internal audit and corporate governance functions. We provide specialist support to the largest public and private organisations in Australia and New Zealand.