AvePoint

MITIGATING COLLABORATION RISK WORKBOOK

How to Build Actionable Plans to Mitigate Risk in Office 365 or Wherever You Collaborate

AvePoint®

Mitigating Collaboration Risk Workbook

How to Build Actionable Plans to Mitigate Risk in Office 365 or Wherever You Collaborate

1

How to Think About Information Risk

What is Information Risk?

Information is the lifeblood of a company. It can give insight into market trends and lucrative new market opportunities.

Information describes performance differences between business units, teams, and individuals. It can record details on customers, prospects, suppliers, and business partners. It drives decision making, the formulation of strategic goals, and the execution of daily tasks by everyone across the organization. Information is valuable and becoming more so.

As with anything of value, information is not risk free. The collection, storage, access, usage, and disposal of information is a breeding ground of risk. And as we have seen in recent events, an ounce of prevention is worth a pound of treatment.

We think about information risk as having two faces: corporate risk and privacy risk.

- ***Corporate Risk.*** Corporate risk is risk to the corporate entity itself, manifested in four ways.

Business risk focuses on the factors that threaten the financial and business viability of the corporate entity.

For example, by using a file share system instead of a robust enterprise communication system with data loss prevention (DLP) functionality like SharePoint, an organization could be at risk of one of its departing employees taking a target client list or other sensitive document over to the competitor that hired them.

Operational risk is about disruption to business processes through ineffectual procedures, failed systems, errors by employees, and fraudulent or criminal activity.

For example, when the City of Atlanta was hit with ransomware in 2018, it spent more than $17 million to restore operations after the attack. Preventing a successful attack from happening in the first place (or having backup data to restore what was stolen) would have been a fraction of the cost.

Reputational risk is that information could be used to cause damage to other people and entities, where the corporation is the source of the damage and thus its reputation is tarnished—with consequential financial damages to revenue, profitability, and market value.

For example, the Cambridge Analytica scandal, which involved harvesting the personal data of millions of Facebook users without the user's consent, has cost Facebook considerable good-will and damage to its brand equity.

Finally, ***legal and compliance risk*** is information that could be accessed, used, destroyed and manipulated in ways that violate the legal mandates and compliance requirements imposed on the corporation.

For example, a defense contractor was fined $75 million for ITAR violations. While its fine was cut in half as a result of deploying AvePoint’s Compliance Guardian to prevent future data leaks, having better information controls from the beginning would have cost only a portion of the nearly $40 million fine.

- ***Privacy Risk.*** Privacy risk is not focused on the corporate entity itself, but rather the people (called “data subjects”) who have entrusted their personal data to another entity.

Privacy risk is that a data subject loses control over their personal information, and that it will be used for purposes beyond what it was given—which can occur within an organization or as a consequence of an organization having ineffectual safeguards around the personal data. Again, the Cambridge Analytica scandal is a good example of a privacy risk and its impact on individuals and the organization.

Drivers of Intensifying Information Risk

Information is increasingly difficult to protect, due to an explosion of more across five dimensions:

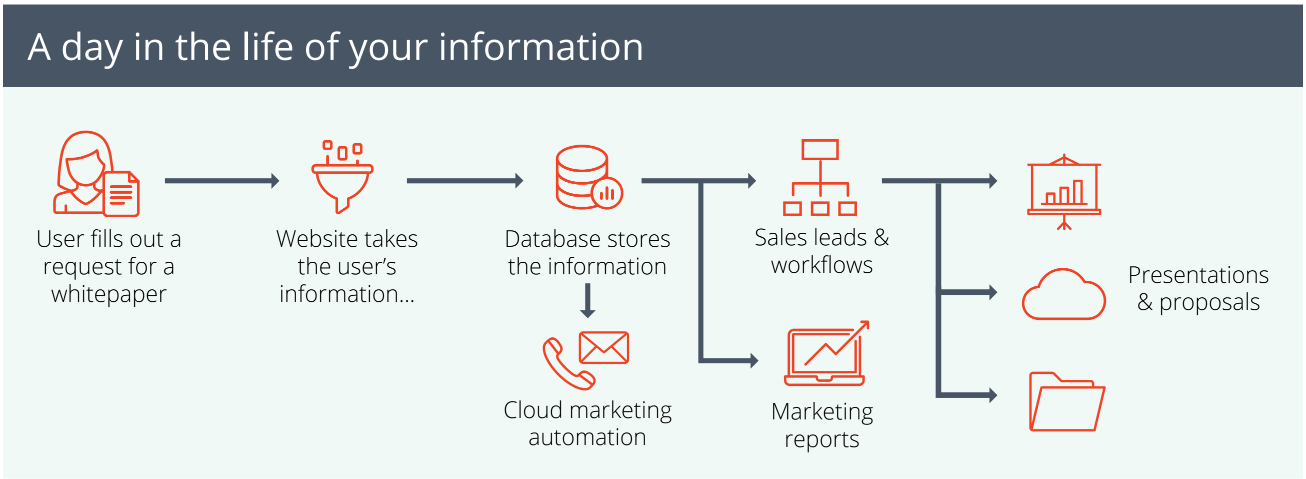
- ***More Data.*** The volume of information available to the world is growing exponentially. Approximately 90 percent of the data that exists in the world today was created only within the past two years (Marr, 2015). That is equal to more than 1.7 quadrillion bytes of data being created every minute worldwide (Domo, 2017). That means there is potentially more sensitive information for organizations to protect every single day.

- ***More Sources.*** New forms of personal data are being created by artificial intelligence and machine learning technologies that enable deeper analysis of patterns of behavior over time for precision profiling and targeting. Modern search engine technologies aggregate, analyze and construct new levels of understanding from data sources originally collected for other purposes. New devices across many Internet of Things (IoT) categories are capturing, creating and storing previously ignored data points.

- ***More Devices.*** Laptops are preferred over desktops, tablets have sold in the hundreds of millions units, the smartphone is the first screen people look at each day, smart watches track everything from exercise to fertility cycles, smart glasses overlay the physical world with point-in-place digital data, and a growing array of IoT devices measure, monitor and act as digital servants at home and abroad. The proliferation of devices storing or providing access to corporate, personal and sensitive data explodes the information risk surface, not just from unauthorized or inappropriate breaches but accidental loss and deliberate theft too.

- ***More Cloud Services.*** Corporates can no longer rely on protecting information through strong network perimeter controls, as the move to the cloud advances and data is stored and accessed beyond the network. On-premises infrastructure as a controlled repository remains vital for most organizations, but with estimates ranging from “dozens” to “hundreds” of different cloud services being used by the average organization, it’s vital to be able to protect information across a growing collection of disparate cloud services.

- ***More Regulations.*** New privacy regulations and compliance standards are springing up across multiple state, country and international jurisdictions. Regional and national standards apply to both the commercial and public sectors in addition to international standards, such as ISO 15489, which outlines global best practices for information creation, capture and management. With additional and changing regulations, there are more risks for potential litigation, and devastating fines for non-compliance.


A day in the life of your information

User fills out a request for a whitepaper
Website takes the user’s information...
Database stores the information
Cloud marketing automation
Sales leads & workflows
Marketing reports
Presentations & proposals

Common Information Risks in Collaboration Platforms

Collaboration platforms can be on-premises such as—SharePoint Server or file shares—or in the cloud like Office 365, G-Suite, Dropbox and Box. Not all sources are created equal when it comes to information risk.

Generally, the substantial investment cloud providers make in their infrastructure security makes the cloud more secure than on-premises solutions. Additionally, some cloud providers like Microsoft have invested in more native security and compliance tools than other vendors.

However, regardless whether your data is in an on-premise or cloud environment, or what vendor you're using, collaboration platforms have common information risks that can be mitigated. These include:

1. Operational risk through constant usage in multiple daily business processes. The relentless frequency of use by employees across the organization increases the likelihood of inappropriate activities, ignored policies, and inadvertent breach.
2. Compliance risk through disparate and non-integrated information protection approaches. While each collaboration platform is likely to offer its own approach for information protection, the organization is left without a holistic approach. The sheer number of different services, each with their own unique protection controls, creates a complex and conflicting control space, which surfaces new information risks rather than dissolving current ones.
3. Unquantified privacy, reputational, and compliance risks due to non-classification of data. Collaboration platforms are used to store, share and give access to unstructured data—including confidential, personal and sensitive data—which is often not classified in collaboration platforms and is therefore without appropriate controls.

Cost of a Data Breach

$141*
Per User ID

$141
Per Document

$141
Per ID Number

$141
Per Email

$141
Per Record

$141
Per Address

$141 Per Record*
Any PII counts as a record

$3,620,000 Per Event
24,000 records on average

*IBM + Ponemon 2017

4. Operational risk through employee selection and usage of collaboration platforms outside the purview of the organization (shadow IT). The Risk and Compliance Department is unaware that cloud services are being used. The Security Operations team doesn't have the ability to capture and respond to security incidents in unidentified cloud services. The IT Department is bypassed and therefore not involved in ensuring appropriate security controls are enacted, such as access controls to prevent breach.

5. Operational and compliance risks due to an expanded set of locations where data responsive to Data Subject Access Requests and Data Deletion Requests is stored (these actions are required by GDPR which is covered in more depth in Chapter 2). Additional locations increase the cost and complexity of response.

6. Compliance and privacy risks through an ever-expanding set of options for sharing data with other people, both inside the organization and external to it. Newly adopted cloud services introduce uncontrolled ways of sharing data, and even sanctioned services such as Office 365 place many different sharing options at the fingertips of users. The proliferation of sharing options increases the likelihood of inappropriate sharing and therefore can cause breach situations.

7. Compliance and privacy risks due to data sprawl and the increased likelihood of inappropriate access, because copies of controlled data and duplicated information are stored without the appropriate controls in place.cause breach situations.

8. Corporate and privacy risks due to third-parties having access to your cloud environments for carrying out system management and administration responsibilities. While personnel from managed service providers, trusted third-party consulting firms, and even the cloud vendor often need administrative access to system controls, they should be prevented by design from having access to the data within the system.cause breach situations.

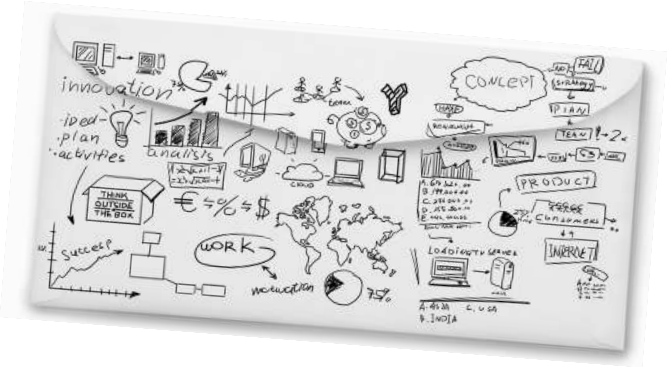
9. Corporate and privacy risks because of having access to third-party data in your environment. Many privacy and data regulations make the entire supply-chain responsible for mitigating information risk. This means you not only need to protect your own organization's data but also the confidentiality, integrity, availability and legal basis of collection of the data from your supply chain as well.

2

How to Measure and Prioritize Risk

Risks are many and varied in nature, and the severity of different risks becoming a reality is no different. In order to initiate informed action to mitigate information risks, we need a structured approach for measurement and prioritization and monetization. Speculative, back-of-the-envelope approaches won't inspire the necessary confidence among decision-makers.

Speculative, back-of-the-envelope approaches include:



- The adoption rates of good security safeguards across an organization's data estate, employees, and guest access population, including strong multi-factor authentication, completed and up-to-date privacy impact assessments, and the use of a cloud access security broker (CASB).
- The risk-adjusted value of avoiding regulatory fines from data breaches and lost devices, using market research for general rates of breach and loss, and current pricing trends from industry analyst firms on the cost of data breaches due to misclassified information.

These are ineffectual because they are uninformed about the actual risks faced by the organization and focus instead on the spread of generalized mitigations. These approaches offer no insight into the specific risks faced by the organization, nor how best to mitigate these risks.

Organizations need to leverage a prescriptive, repeatable and mathematical approach to risk management. Using such an approach to quantify and mitigate risk demonstrates intentional corporate action to deal responsibly with risk, which can soften the hard edge of legal and regulatory action. Our approach has six steps:

1. Identify the risks you face.
2. Determine the likelihood of being impacted by each risk.
3. Calculate the severity of being impacted by each risk.
4. Visualize the risk portfolio by plotting likelihood against severity.
5. Decide mitigations for the risk portfolio.
6. Implement measures for auditing the risk portfolio over time.

Let's take a look at each step.

Step 1 Risk Identification and Surfacing: External Regulations and Internal Policies

Knowing the risks you face is step 1. Surfacing, identifying, describing and categorizing these risks puts the initial shape to your specific situation, and then informs what you need to do about these risks.

Most organizations face risks across two broad groupings: external regulations that demand a standard of protection for information (along with punitive measures for non-compliance), and internal policies and best practices. Let's look briefly at each in turn.

Type 1 **External Regulations.** There are a growing number of significant regulations that set expectations on how personal and sensitive data should be protected across the APAC region. These regulations include punitive regimes to dissuade non-compliance.

Data Protection and Security trends in the APAC Region. As in the rest of the world, the APAC region is facing mounting pressures that come from collecting, creating, using and appropriately sharing and protecting critically sensitive data. As organizations develop and implement their infrastructure consolidation, and cloud strategies, this creates additional challenges for balancing access to information that should be available and protection of information that should not be available.

Moreover, the average person is now familiar with security. Breaches appear on the nightly news and as a consequence, citizens are more "security aware" today than they ever have been in the past. Not only is there a heightened awareness level among citizens and their concerns about theft, fraud and security, but also there is a change in the policy and regulatory landscape.

The Impact of the EU GDPR in APAC. The GDPR, implemented in the EU in May 2018, continues to impact multinational organizations, including those headquartered in the APAC region. Primarily, this has been because of the expanded applicability of European data protection law from an "establishment" concept limiting the law's application to organizations with "bricks and mortar" operations on the ground in the EU to a broader set of criteria making the GDPR applicable to APAC businesses. The prospect of penalties reaching 4% of world-wide turn-over has caught the attention of many APAC-based businesses, APAC based companies need to carefully consider their operations and interactions with the EU and EU data subjects.

GDPR has also inspired some modifications across established data protection regimes in the APAC region, such as those in Australia, Hong Kong, New Zealand and Singapore, which have been selectively implementing "GDPR-like" requirements, such as mandatory data breach notifications and obligations focused on ensuring greater accountability. Emerging data protection laws, such as those being introduced in India, are poised to take a substantial leap from very limited regulation to GDPR-inspired comprehensive regulation.

Australia. Australia regulates data privacy and protection through a mix of federal, state and territory laws. The Federal Privacy Act 1988 (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies. Under the Privacy Act, the Privacy Commissioner has authority to conduct investigations, including own motion investigations, to enforce the Privacy Act and seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts.

Most states and territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to state government agencies, and private businesses that interact with state government agencies. These acts include: Information Privacy Act 2014 (Australian Capital Territory) Information Act 2002 (Northern Territory) Privacy and Personal Information Protection Act 1998 (New South Wales) Information Privacy Act 2009 (Queensland) Personal Information Protection Act 2004 (Tasmania), and Privacy and Data Protection Act 2014 (Victoria).

Australia continues to review its Privacy Act, with fresh impetus in 2019 off the back of the Digital Platforms Inquiry led by the Australian Competition and Consumer Commission (the "ACCC"). The Office of the Australian Information Commissioner will be taking forward a recommendation to implement a new binding Privacy Code for digital platforms and increased penalties for privacy breaches, amongst other potential reforms, although there are reports that legislative reform of the Privacy Act will not be complete until 2021. Australia has made significant moves to upgrade its Privacy Act in recent years, and the focus now appears to be to make the law fit for purpose for a rapidly advancing digital economy. The ACCS's separate Consumer Data Right initiative promises a vision for consumer data sovereignty to improve competition across a range of industry sectors, including financial services and telecommunications. The API-powered vision of data portability is a striking move, but will of course raise the stakes from a data privacy point of view. With this in mind, the potential fines for breaches of the Privacy Act would increase from a maximum of A$2.1 million (USD 1.4 million) for serious or repeated breaches, to the greatest of: (i) A$10 million (USD 6.9 million); (ii) three times the value of any benefit obtained through the misuse of information.

New Zealand. New Zealand is in the process of updating its Privacy Act, with the changes expected to come into effect in December of 2020. The new Act retains the privacy principles of the current legislation, with some changes. Principle 1 has been clarified to ensure that businesses and organizations do not collect identifying information from people if it is not necessary. The updated Act will allow the Human Rights Review Tribunal to award up to $350,000 to each member of a class action, resulting in potential significant monetary fines.

Singapore. Singapore signed its Cybersecurity Bill into law in February 2018, and it provides a framework for data privacy for information infrastructure providers. Singapore's Personal Data Protection Commission (PDPC) is also considering adding a mandatory breach notification as well as relaxing the consent requirements on data controllers.

Singapore's push to be a leading regional innovation economy is reflected in the rapid pace of regulatory development of the Personal Data Protection Act (the "PDPA") and the thought leadership of the Personal Data Protection Commission (the "PDPC"). The authority has also been very active investigating complaints, most significantly with respect to the Singapore health system breach in 2018, which reportedly compromised the personal data of 1.5 million Singaporeans.

Japan. The Act on the Protection of Personal Information ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission (the "PPC"), a central agency acts as a supervisory governmental organization on issues of privacy protection. The APPI was originally enacted in 2003 but was recently amended and the amendments came into force on 30 May 2017.

The Japanese government and the European Commission have been working together on data privacy to create operational efficiency for global business. As of January 2019, they have formalized a framework for the mutual and smooth transfer of personal data between Japan and the EU.

Penalties for misusing personal information for unlawful gain face imprisonment for at least a year and/or a fine of 500,000 yen. In April 2019, the Personal Information Protection Commission of Japan (the "PPC") published an interim report on its review of the Act on the Protection of Personal Information (the "APPI"), proposing that the APPI, which was last amended in 2017, be amended to introduce a mandatory data breach notification obligation, a right of data portability, strengthened regulation of cross-border transfers, stiffer penalties for contravention (including administrative fines) and the introduction of "big data" reforms concerning anonymization and the processing of pseudonymized personal data similar to reforms introduced in South Korea.

China. There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal data protection and data security are part of a complex framework and are found across various laws and regulations. Provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law have generally been used to interpret data protection rights as a right of reputation or right of privacy. However, such interpretation is not explicit.

On June 1, 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cybersecurity and data privacy protection.

The Cyber Security Law of the People's Republic of China, commonly referred to as the China Internet Security Law, was enacted to increase data protection, data localization, and cybersecurity in the interest of national security to increase cybersecurity and national security. The law is applicable to network operators and businesses in critical sectors, such as telecom, information services, energy transport, water, financial services, public services and digital government services.

In practice, the law is applicable to almost all businesses in China that manage their own email or data networks. Network operators are expected to clarify cybersecurity responsibilities in their organization, safeguard network operations, prevent data leaks and theft, and report any cybersecurity incidents to the users as well as the relevant government department for that sector. The law also provides regulations and definitions on legal liability, including punishments.

Hong Kong. Hong Kong's Privacy Commissioner for Personal Data (the "PCPD") remains a policy-making leader in the region. The government and the PCPD have been working towards improvements to the Personal Data (Privacy) Ordinance (the "PDPO"), a comprehensive data protection law which has only been amended once since its introduction in 1995. The Personal Data Privacy Ordinance, established in 1995, protects the individuals in relation to their personal data. Personal data is widely defined. It is any data that directly or indirectly relates to a living person. The law applies to any organization that controls, processes or holds personal data in or from Hong Kong. Data breach notification is voluntary.

Type 2 **Internal Policies, Contractual Commitments and Best Practices.** Although external regulations impose requirements on action and create information risks, a second source of risk flows from internal policies and best practices. Such policies are likely to address areas such as:

- Protections around commercially-sensitive information including intellectual property, business secrets, business plans, merger and acquisition activities, patents under development, and future research projects. Knowing in general what needs to be protected must be matched with the ability to capture and classify information that fits in each of these categories.

- Controls to limit what third-party IT providers can do within systems that contain commercial, personal and sensitive data. While third-party providers will need access to the management and administrative capabilities of systems to carry out their assigned tasks, they should have no standing access to the data in such systems and carefully controlled processes should be in place to enable data access only when absolutely essential. Risks of this nature can be inferred from the regulations above, but it is also just good business practice to tightly manage access controls and permission rights for anyone with access to your systems.
- Understanding the nature of any contractual commitments you have made to your customers and/or employees with regards to risk management, privacy protections and security is also critical.

Impacts of ignoring internal policies and best practices include:

- Business risk due to loss of competitive advantage, resulting from the theft of commercially-sensitive information. In the wrong hands, such information can undermine the ability for an organization to meet its business and financial goals.
- Reputational risk due to customer's learning about a data breach of the organisation's own commercial information, creating concerns about the potential lack of safeguards on personal and sensitive information belonging to clients.

Step 2 Determine Likelihood

The likelihood of a risk becoming an actual event is the first of two critical questions to ask about each risk. Some risks are highly likely to occur given the new culture of teamwork and sharing taking root across the world.

Without the appropriate mitigations in place, risks with near certainty of happening include personal or sensitive data being shared with unauthorized people, phishing and spear-phishing messages being clicked leading to credential theft, and new cloud collaboration services being used by employees without appropriate oversight by corporate IT.

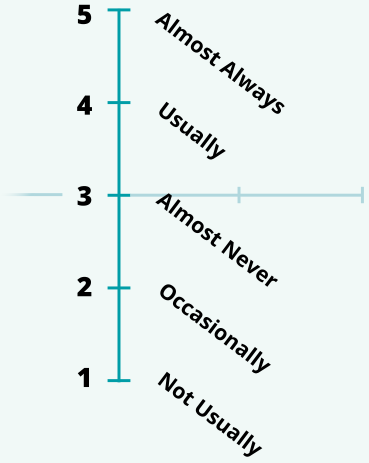
Other risks have a lower likelihood of occurrence, such as a successful ransomware attack that encrypts all data sources in the organization.

Tools for developing a sense of the likelihood of being impacted by each risk include:

- Market research on general cross-industry trends and incidents, such as the general rate of phishing attacks on organizations of all kinds.
- Industry-specific research on risk rates for your industry. For example, we know that the government, healthcare and education sectors are heavily attacked by external threat actors.
- The number of shadow IT services being used among employees instead of corporate sanctioned services. The greater the number of services used the higher the likelihood of breach.
- Current mitigations that your organization already has in place, such as Advanced Threat Protection services in Office 365 or from another vendor to reduce the likelihood of compromise through malicious attachments and links.
- The number of third-party business partners who have trusted relationships with your organization, and the risk maturity for each one. Low risk maturity scores from many partners will increase the likelihood of a risk being triggered.
- The correlation between internal employee satisfaction survey scores and the departure of disgruntled employees to competitor firms. If there's a pattern, such employees may be creating ways of stealing corporate information.

For the purposes of this eBook, we advocate using the following rating scale for likelihood:

LIKELIHOOD



Step 3

Calculate Severity

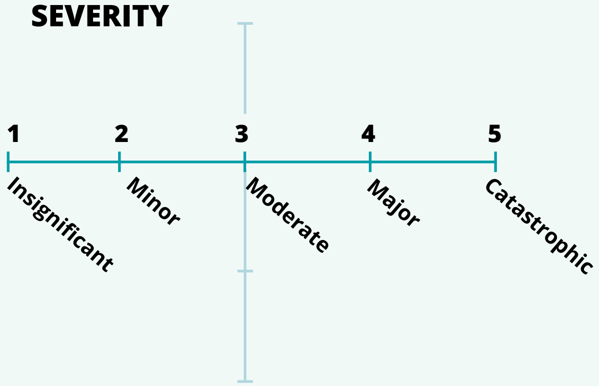
The severity of a risk becoming an actual event is the second critical questions to ask about each risk. Some risks carry CEO-goes-to-jail or go-out-of-business level severities, but most rank lower on the scale.

Privacy risks subject to administrative fines under the growing armada of global privacy regulations threaten significant financial fines, such as the oft quoted 4% of global annual revenue under the GDPR.

Depending on the type and nature of your data and systems, and whether appropriate mitigations are already in place, a successful ransomware attack can rank from low to critical on the severity rating scale.

For the purposes of this eBook, we advocate the following rating scale for severity:

SEVERITY



Step 4

Visualize the Portfolio

Plotting each of the risks on a heat map using likelihood and severity as the axes enables a visual representation of criticality and priority. The intersection of five rating levels for likelihood and five rating levels for severity results in a 5 x 5 matrix with 25 individual plot options.

Risks that plot into the low areas of the heat map can be treated differently to those that plot into the medium, high and critical areas.

While risks are multitudinous, the resources to mitigate each are usually constrained in each time period and therefore prioritization is essential to ensure limited resources are invested in the right places. Right, in the sense used here, is about responsiveness to the highest priority risks balanced against the cost and complexity of the proposed mitigations.

Step 5 Decide Mitigations

Armed with a prioritized risk portfolio, investigate and decide on mitigations to pursue immediately, in three months, in six months, and beyond. Mitigations could include the following, for example:

- To reduce operational risk, migrate away from certain cloud collaboration platforms to one of the corporate sanctioned services, such as Office 365. Reduce the number of places where people work together, and store information to tighten the ability to exert control.
- To reduce privacy risk, implement a cloud access security broker (CASB) to apply data protection mechanisms to data stored in cloud services, track potential credential compromise through anomaly detection, and audit the security settings on cloud services, among others.
- To reduce reputational, compliance and privacy risks, implement stronger authentication mechanisms including strong multi-factor authentication.
- As a general mitigation, employee awareness training on the different types of information risk, along with actions to take to reduce the likelihood of converting a risk into an actual event. Awareness training helps with cultivating a human layer of protection and risk mitigation, because employees know what they should and shouldn't do.

We will consider potential mitigations in greater detail later in this eBook, but the other concept to call out now is our 30:60:90 days roadmap—which essentially adds the third dimension of time to the risk heat map.

The third dimension provides a structured way of starting to embrace the planned mitigations, but without the demand to do everything immediately. It designs experimentation, learning, initial results, and ongoing improvements into an achievable plan.

Over three consecutive time periods of 30 days, our roadmap says:

- **Days 1-30.** Focus on quick wins and initial achievements. For example, locate personal and sensitive data across all the collaboration platforms and other storage locations connected with your organization.

  Note where external sharing is happening currently, or where information is made available to everyone within the organization. Secondly, architect a classification scheme for personal and sensitive data, so that labels can be applied to each content item that describe the types of personal and sensitive data contained inside each one.
- **Days 31-60.** Deepen the efficacy of your initial work. For example, modify how personal and sensitive data is identified based on learnings from the initial 30 days. This may include creating several custom definitions to get at the data types commonly used in your organization. Additionally, your classification scheme should be ready to move to automated application, with the option of human review.
- **Days 61-90.** Ensure the ongoing management and reporting of your mitigations are performant, including, for example, monitoring for leaks of personal data, and aggregating incidents for longer term integrated reporting and analysis.

Step 6 Ongoing Risk Auditing and Updating / Incorporating Newly Identified Risks

Once the initial mitigations have been implemented, ongoing measurement is essential to ensure the mitigations are having the desired effect.

As soon as it is determined that current mitigations are not working, alternatives must be identified and put into play. Risk mitigation is not a matter of single one-time actions, but rather the development of a culture of appraising, rating and controlling risks.

3

Common Risks

We have briefly introduced the concept of information risk and looked at its various sub-types. We have explored how to take a structured approach to measuring and prioritizing risk. In this section, we look at a long list of risks we commonly hear from our customers.

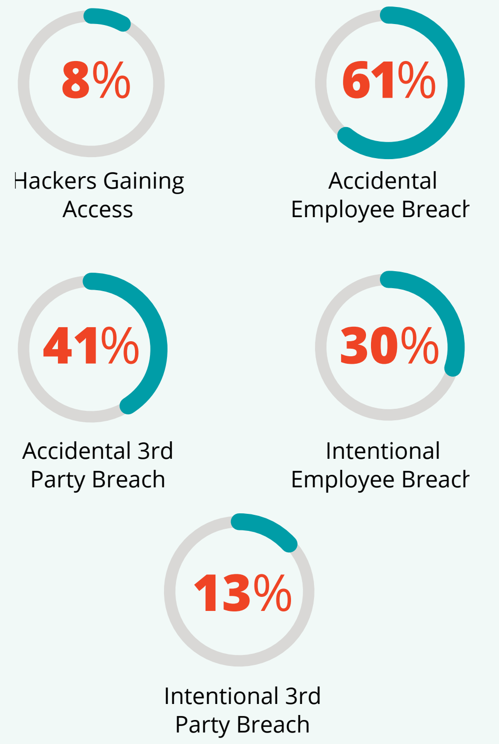
While we don't expect that you face every single one of these risks, we do expect that you face many of them. For each risk identified in this section, we have given our general sense of likelihood and severity. Our sense is a general perspective and may differ widely from your own rating.

Each collaboration platform and cloud service will have their own set of security and compliance tools, but where applicable, we have included relevant ways to address these risks using native Office 365 tools.

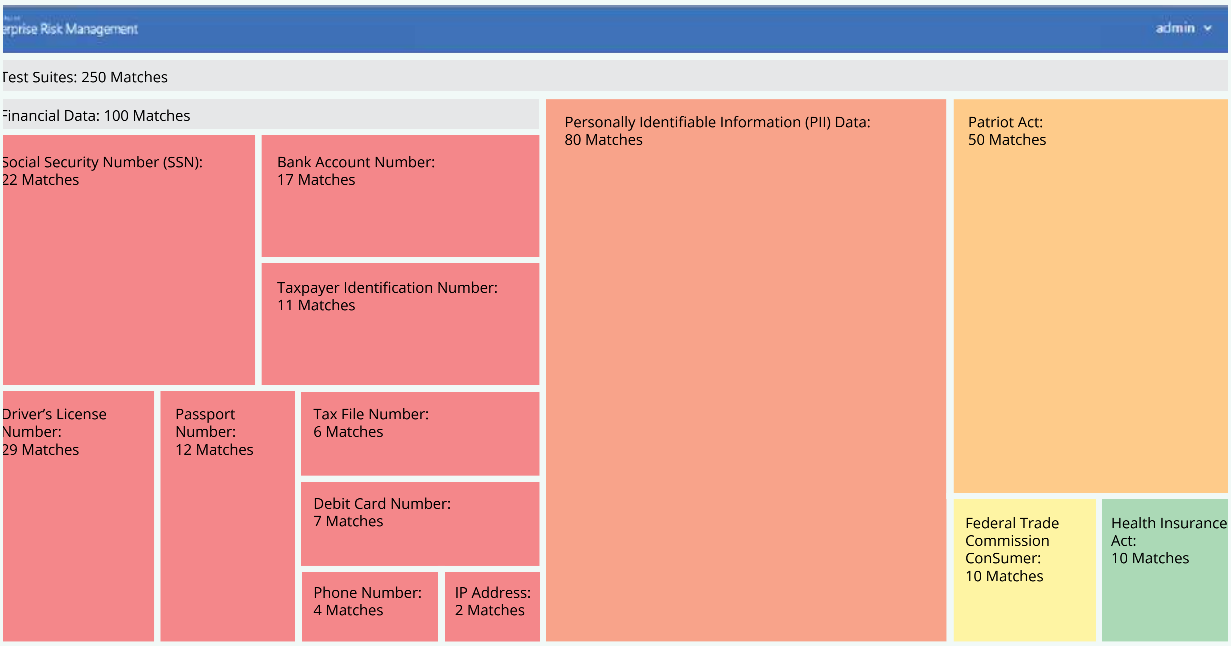
This is because it is the most widely used cloud collaboration platform and it has the most advanced security and compliance features.

It is important to keep in mind that not all data will be in Office, your organization may leverage multiple clouds, or there will be instances where you need extended functionality. As such, we also briefly highlight relevant AvePoint functionality across these risk areas.

How likely do you think the following privacy breach risks are?



Scan your content for PII and sensitive information.



Test Suites: 250 Matches

Financial Data: 100 Matches

Social Security Number (SSN): 22 Matches

Bank Account Number: 17 Matches

Taxpayer Identification Number: 11 Matches

Driver's License Number: 29 Matches

Passport Number: 12 Matches

Tax File Number: 6 Matches

Debit Card Number: 7 Matches

Phone Number: 4 Matches

IP Address: 2 Matches

Personally Identifiable Information (PII) Data: 80 Matches

Patriot Act: 50 Matches

Federal Trade Commission ConSumer: 10 Matches

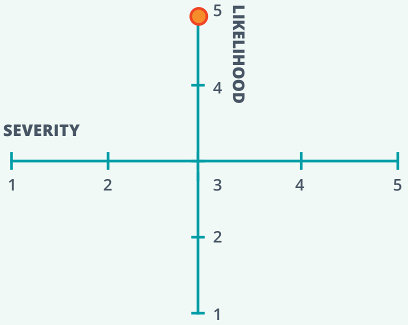
Health Insurance Act: 10 Matches

Unclassified Data.

Aspects of this risk include internal and external people inadvertently gaining access to sensitive data they should not have access to, or data that should be retained is deleted unwittingly. A third aspect is when duplicates of such sensitive data is stored on or accessible through mobile devices with weak device controls that are lost or stolen.

Office 365 has sensitivity labels and robust data classification functionality. AvePoint Policies and Insights (PI) can highlight (and even auto-correct) high-risk scenarios where sensitive content has "shadow users" where its being shared with anonymous links or more broadly than appropriate.

If you have data outside of Office 365, and chances are you do even if you don't know it, then Compliance Guardian's data validation and classification module can help.

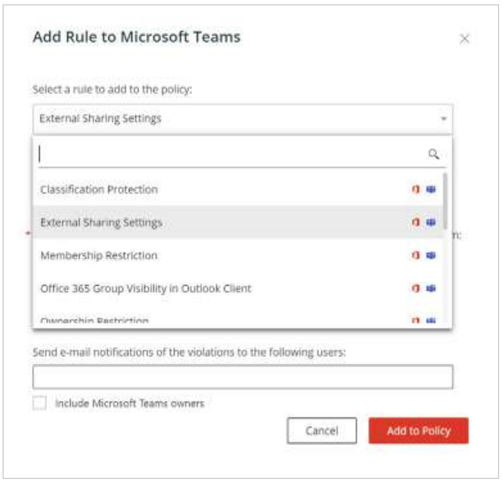


In terms of plotting the risk, our view is:

- The likelihood is Almost Always (5), meaning that almost every organization has unclassified data across its data estate.
- The severity is at least Moderate (3), but that could be higher (or lower) depending on the specific types of data that are unclassified and the impact on the organization as a result of breach or unwitting data destruction.

Risks with External Sharing and Guest Access.

With the increasing embrace of short-term contractors, client portals, and collaboration platforms shared with business partners, external sharing and guest access to corporate data is commonplace.



Add Rule to Microsoft Teams

Select a rule to add to the policy:

External Sharing Settings

- Classification Protection
- External Sharing Settings
- Membership Restriction
- Office 365 Group Visibility in Outlook Client
- Ownership Restriction

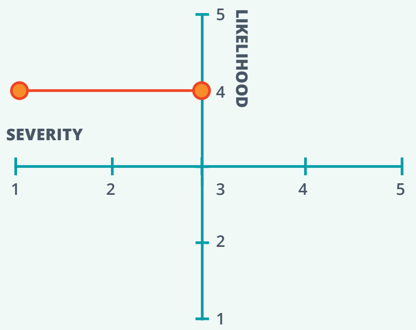
Send e-mail notifications of the violations to the following users:

□ Include Microsoft Teams owners

The risk, however, is that external sharing rights are set too broadly, enabling people outside the organization to gain access to personal, sensitive and confidential data they should not see.

This creates a breach situation which can be related to either corporate or privacy risks, depending on the nature of the information thus breached.

Office 365 has numerous settings that can provide data surrounding external sharing and guest access, almost too much. AvePoint PI can surface and prioritize high-risk scenarios in your environment including which pieces of sensitive content have been shared by which users with which external users and with what frequency.



- **The likelihood** is generally a Usually (4), although we'd prefer it to be an Almost Never (1). Likelihood rates this highly because there are just so many different systems in use, with easy at-your-fingertip controls for external sharing, that it must happen daily for the average organization.

As one data point, when the White House analyzed the cyber incidents across the U.S. government in 2015, it found 77,000 incidents in total, but commented that only a small number were significant data breaches.

Among the vast majority would be many cases of external sharing gone wrong, either through email or other sharing services. If we assume 100 significant data breaches, then 76,900 incidents over a year gives an average of 210 less significant incidents per day.

- **The severity** of inappropriate external sharing and guest access is trending upward, driven by new global data protection regulations such as GDPR. On average, severity has been at an Insignificant (1) level for an organization, but the growing privacy rights of people is pushing severity toward the Moderate (3) range.

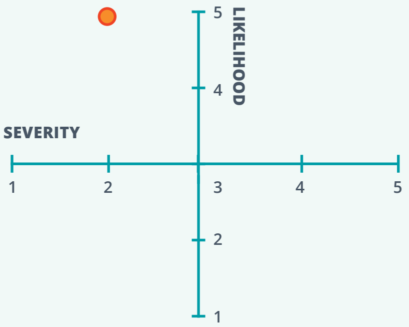
Shadow IT Creates Unquantified Information Risk.

Microsoft estimates that the average large organization has over 100 IT-managed applications, and at least another 900 apps that are outside the purview of the IT department.

The type of content stored in these shadow IT services vary widely, but must include a smattering of business confidential, personal and sensitive data.

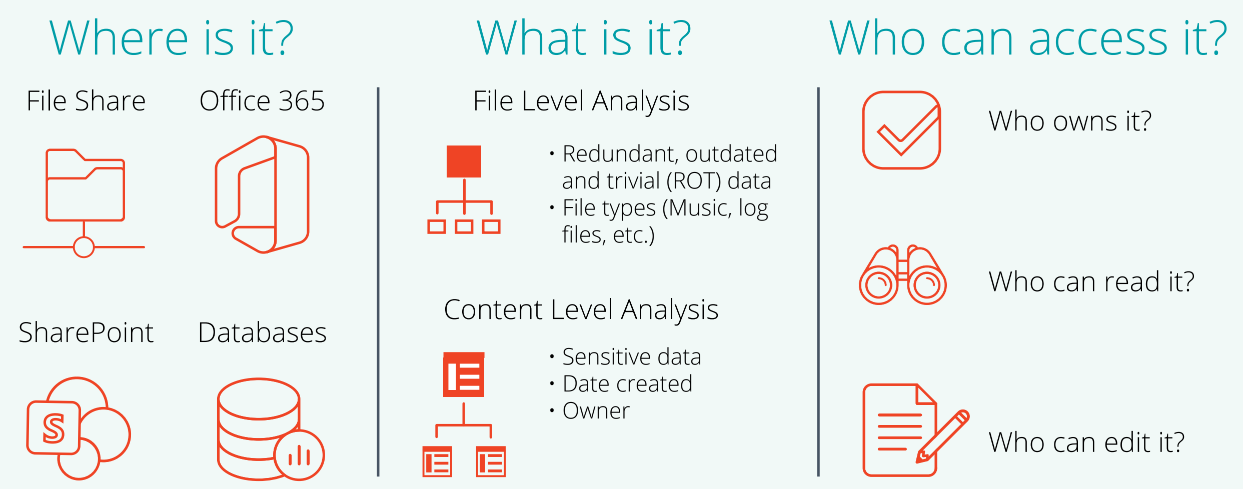
Apart from the baseline storage of such data in shadow IT services, a related risk is misconfigurations or security vulnerabilities in cloud services that permit unauthorized access and breach.

Office 365 has tools (for Enterprise Mobility + Security users) such as Cloud Discovery that can help you identify shadow IT and what cloud apps are being used within your organization. AvePoint also has a tool that can help identify shadow IT and map how your data flows across your organization.



- **The likelihood** rates at Almost Always (5), because very few organizations have completely prohibited and prevented the access and usage of non-sanctioned services. With the barrier to adoption being so low, due to services often having an initial free tier, employees are quickly able to embrace the next hot service without regard to IT policies.
- **The severity** is at the Minor (2) level in many cases, although there are situations where severity ranks higher if vast quantities of data is breached. Organizations are generally fast to respond to a notification of an open shadow IT service, and the ramifications for the organization are generally short-lived. This may change as global data protection regulations start having an impact through administrative fines and other sanctions against offenders.

Determine data flow, connections to other data or systems, and conduct impact assessment for security & privacy risk insight.



File Level Analysis

- Redundant, outdated and trivial (ROT) data
- File types (Music, log files, etc.)

Content Level Analysis

- Sensitive data
- Date created
- Owner

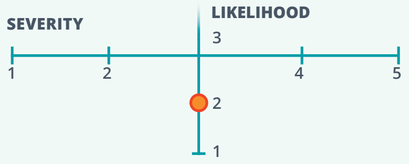
Backup System Failures.

Backup systems that are inappropriately secured, inadequately scoped, or insufficiently robust create information risks for an organization. Inappropriately secured backups create the risk of data breach, as happened to the rsync backup server at the Oklahoma Securities Commission in early 2019, exposing millions of files containing sensitive data in a 3 TB data set.

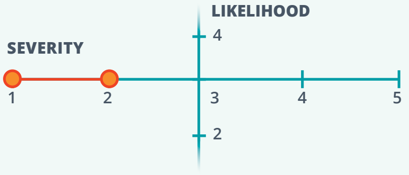
Backups that are inadequately scoped or insufficiently robust become a problem when data needs to be recovered, such as through accidental deletion, system failure, or a ransomware attack that disrupts access to all corporate data on production systems.

Some organizations compromised through a ransomware attack or from an insider error (either benign or malicious) who have performant backup systems have been able to recover quickly. AvePoint Cloud Backup leverages Azure to ensure a high degree of availability for backup data—beyond the standard 93-day retention period for deleted Office 365 data—as well as quick restore times.

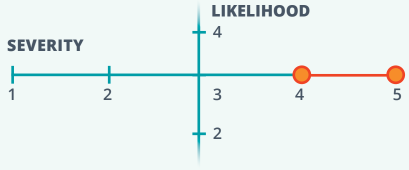
Others without such protections have struggled to recover, spent extravagantly to mitigate after-the-fact, or in several cases, gone out of business entirely.



- **The likelihood** of a data breach occurring via an inappropriately secured backup system is about a Not Usually (2), but with a **severity** of at least a Moderate (3), although that will be lower if there is no personal or sensitive data breached.



- **The likelihood** of needing to recover a missing file ranks at about an Occasionally (3) level. In terms of **severity**, the inability to recover a missing file is generally at a Minor (2) or Insignificant (1) level.



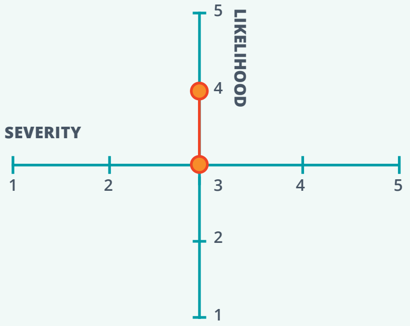
- **The likelihood** of backup system failure at an inopportune moment or full encryption of production systems via ransomware when no backup is available, for any given organization, rates at a likelihood of Almost Never (1). But **severity** is at the other end of the scale. If this situation does happen, severity is at least a Major (4) if not a Catastrophic (5).

Information Used in Unauthorized Ways.

The use of information in ways beyond the initial intent, legal basis, or scope of consent from the data subject creates risk situations.

A departing employee taking a list of customers with them to their new job of a competitor triggers several types of corporate risk and privacy risk. Facebook use of customers' mobile phone numbers for advertising purposes, a use excluded from the initial consent scope of security verification, triggered a compliance risk.

Any time an organization builds a mailing list from a customer database where consent was not given for marketing purposes triggers a potential compliance and privacy risk.



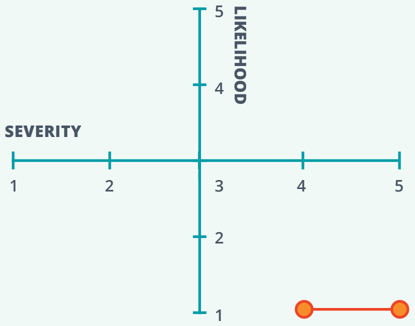
- **The likelihood** is a Usually (4), due to poor information practices at organizations necessitating new global privacy regulations to rein in bad behavior. As regulations such as the GDPR and CCPA start to bite, we expect to see the likelihood decrease a step to an Occasionally (3).
- **The severity** is at most a Moderate (3), unless the use of information in unauthorized ways is a core tenet of the organisation's business model and widespread misuse is commonplace in which case the severity will rate higher.

Records Not Retained.

Business records that should be retained are inadvertently deleted, stored in an inappropriate location (e.g., an employee's OneDrive account that gets deleted 30 days after they leave the organization), or are compromised in a ransomware attack.

Office 365's native records management tool and its label functionality can help automate this process so that its less dependent on end users. AvePoint record solutions can help extend this functionality to physical records and hierarchical taxonomies as well.

If the number of records that are not retained is low—such as through an employee not following business processes for record retention—the overall severity will be minor. If we exclude this case from our analysis and focus on the widespread compromise of records through inadvertent deletion or a ransomware attack, then:

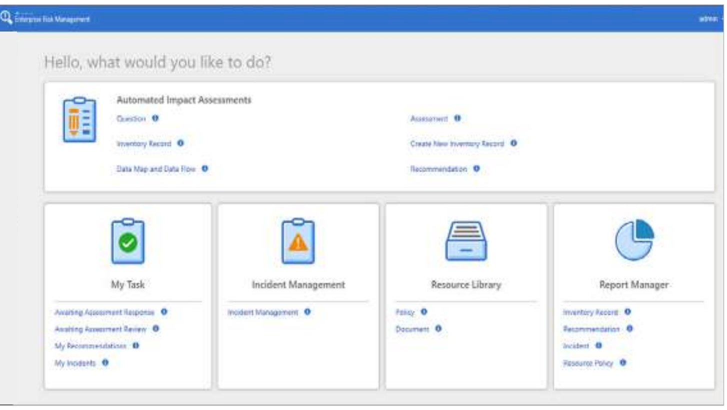


- **The likelihood** is an Almost Never (1). It does happen now and then, but the cases are rare.
- **The severity** rates between the mid—and high-levels on the severity scale and is impacted also by the industry affiliation of the organization. Lack of access to vital patient health records, for example, rates at the higher end of the scale for a healthcare provider. Likewise, for city municipalities and other entities in the government sector who are unable to access production systems and historical records.

Supply Chain Risks.

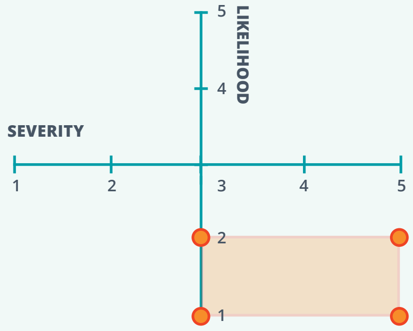
The other firms in your supply chain face information risk of their own, and the triggering of risks in these firms can impact your corporate and privacy risks.

For example, if you outsource your core business systems to a third-party provider who gets compromised through a ransomware attack—as happened in mid-November 2019 for an IT outsourcer to 110 healthcare facilities in the United States—the impact can be catastrophic if access to your core systems and data is disabled.



Another risk scenario, albeit generally with a less than catastrophic severity, is when employees at your managed service provider have access to both your system and the data contained inside; system access for configuration changes is required, but access to data inside the system should be prevented by design. Compliance Guardian can help security teams automate and accelerate their internal and third-party impact assessments.

If strong controls are not in place to create hard boundaries between the two, third-party personnel may have access to the personal, sensitive and confidential data under your jurisdiction.



- **The likelihood** is between an Almost Never (1) and Not Usually (2). It happens sometimes—through errant third-party employee behavior or a once-in-a-hundred-years digital storm. The triggering of supply chain risks makes major headlines, because many organizations find themselves blindsided by such occurrences.
- **The severity** is at least Moderate (3), and in some risk scenarios a Catastrophic (5). Severity depends on the types of transferrable information risks in your supply chain that could impact your organization, which can only be answered through a due diligence process. If your organization has all its data stored with non-first-tier cloud providers or outsourcing firms who could be subject to a ransomware attack, the severity pushes toward the Catastrophic (5).

Malicious External Threats.

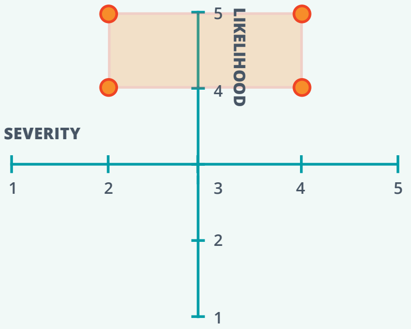
Information is a valuable commodity, and external actors are actively seeking ways of stealing value from organizations. For external actors with malicious intent, value can be gained by stealing confidential (e.g., intellectual property), personal and sensitive data and using it directly, or for its resale value on the dark web.

A successful ransomware attack can result in a ransom payment, especially as insurance companies seem increasingly willing to pay ransom demands, and stock market movements in response to a data breach notification or regulatory fine can enrich shrewd stock manipulators.

Almost all organizations are being hit with non-malware attacks, such as the relentless phishing and spear-phishing attacks that often seek out account credentials to enable a security breach.

Office 365 has a variety of tools to protect your organization against phishing attacks, including an attack simulator. The platform also provides Advanced Threat Protection (ATP) that allow organizations to define threat-protection policies, investigate threats, and automate breach response.

And external actors are quick to leverage software vulnerability notifications from vendors to compromise unpatched systems, sometimes for immediate gain through data exfiltration or ransomware, and at other times to move laterally through a network gaining ever more control points for a future coordinated attack on a grand scale.



- **The likelihood** of malicious external threats being targeted at organizations is in the Usually (4) or Almost Always (5) range. Such threats are ever-present, ever-changing, and ever-damaging if they successfully snare a victim.
- **The severity** is in the Minor (2) to Major (4) range in general, depending on the nature of the threat, the extent of the compromise, and the overall health of the organization. For example, the £99 million fine against Marriott for the data breach of personal information on 383 million guests is a lot of money, but nothing that will cause significant financial harm to the firm beyond a short-term blip.

  But severity can be higher or lower too. Sometimes a threat is triggered too early to cause significant damage, and the impact is minimal. And in a few instances the impact is catastrophic, such as the data breach at Retrieval-Masters Creditors Bureau in August 2018 that led to a Chapter 11 filing in mid-2019. But on average, the severity is somewhere in the middle range.

Maleficent Insiders.

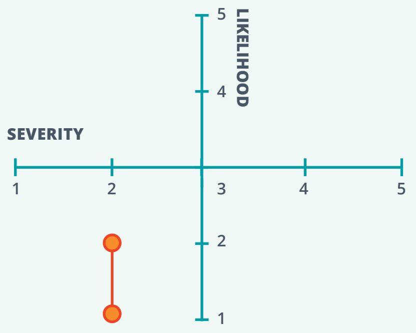
Some employees use the guise of good corporate citizen to cover more maleficent purposes including espionage, data theft, and accomplice to data exfiltration to an external threat actor.

The options for carrying out such motivations are widely available, from email attachments to personal cloud file sharing services to corporate-friendly shadow IT services and the ever-present “Share” button in Office 365.

The scale of theft incidents varies widely, from the recruitment consultant in the United Kingdom who stole the contact details on around 100 existing and potential clients when she joined a rival agency, to the employee at Trend Micro who stole data on 68,000 customers for resale to a third party, and the employee at SunTrust Bank who stole account details on up to 1.5 million clients.

Deliberate insider theft makes up the lowest category of insider threat risks, with negligent or accidental exposure over three times more likely to happen, but it remains a threat and a risk, nonetheless.

Office 365 has data loss prevention and information rights management settings that can mitigate risks from maleficent insiders.



- **The likelihood** of high-profile maleficence is at the Almost Never (1) level, while deliberate theft slightly higher at Not Usually (2).
- **The severity** to the organization generally rates somewhere between Insignificant (1) and Moderate (3), depending on the scope and scale of the resulting theft. For averaging purposes, we will rank it as Minor (2), because even if fines are levied against the organization for inadequate security controls, criminal proceedings can be taken against the individual or individuals involved.

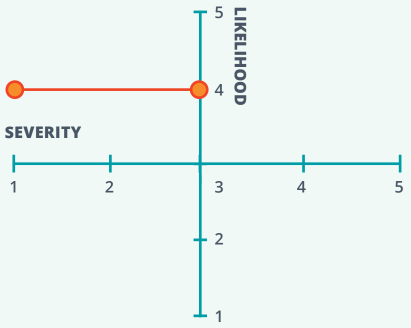
Mobile Devices for Data Theft.

The increased proliferation of small form factor mobile devices with large local storage facilities or remote access to corporate data repositories creates a variety of corporate and privacy risks.

If unmanaged personal mobile devices are used for corporate purposes, a departing employee may retain access to corporate repositories after their employee has been terminated.

Or if personal mobile devices lack a passcode and have access to corporate data through sync or apps, corporate data can be breached if the device is lost or stolen. One research study found that of 70 million devices lost every year, only 7% are returned or recovered, thereby creating a 63 million device differential every year.

And it’s not just smartphones and tablets that are at risk, because even a USB memory stick can contain personal and sensitive data. Microsoft has several solutions that can help mitigate risks from mobile devices within its Enterprise Mobility Security offering such as its Intune unified endpoint management solution.

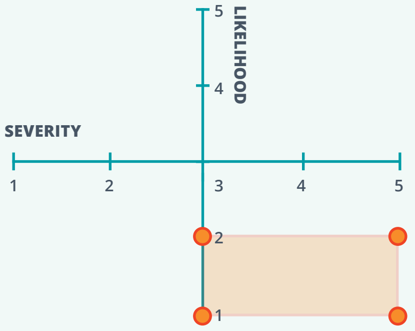


- **The likelihood** is Usually (4), given the high number of devices that are lost or stolen every year—including mobile phones, tablets, laptops, and USB memory sticks.
- **The severity** is generally at the Insignificant (1) or Minor (2) end of the scale, although newer data protection regulations may result in higher and most costly administrative fines being levied. In average situations, this could raise the severity to a Moderate (3) at most.

Unavailability of Information.

Article 32 in the GDPR requires organizations to have "appropriate technical and organizational measures" to, among other things, ensure the ongoing availability and resilience of processing systems and services.

When a malware or ransomware attack compromises system and information availability, the organization falls afoul of this GDPR requirement. Again, a third-party backup solution can help mitigate this threat.

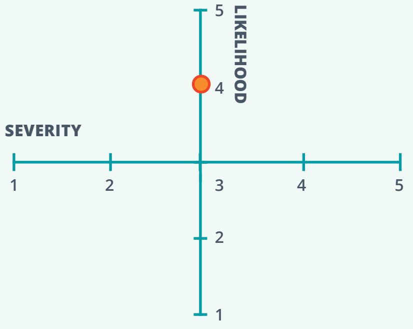


- **The likelihood** is around an Almost Never (1) and Not Usually (2), even though such attacks generally claim the headlines when they successfully land.
- **The severity** is in the mid—to high-range for a successful attack, depending on the scope and scale of the compromise and the type of information processing systems that are rendered unavailable. If easy mitigations exist to restore availability, then severity is greatly lowered. If mitigations are non-existent or fail, then severity tends to push towards the higher end of the scale.

Fog Hides Insight.

In a recent study, Ponemon found that over half of organizations did not carry out post-deployment monitoring to assess the efficacy of investment in cybersecurity tools and solutions.

Data is moving faster than ever and its hard for security teams not to be paralyzed by the hundreds of minor violations within an environment. By the time the IT or security team pulls a report, it could already be outdated. Its important to have tools that don't just catalogue every possible infraction or lock down environments until they are unusable, but that prioritize the areas that will impact your risk levels. Otherwise you will be a hamster in a wheel, scrambling but without much progress being made.



- **The likelihood** is a Usually (4), since Ponemon found that over half of organizations did nothing to gauge efficacy post-deployment. This is the usual state of play on average across organizations, although almost half of organizations did monitor efficacy.
- **The severity** lands, on average, in the middle of the range, so something like Moderate (3) would best describe the consequence of such fog. A lack of visibility can enable information risks to fester.

4

Mitigation Action Plan

Mitigating information risks in any organization relies on two core principles: first, make it easier for end users to do the right thing than the wrong thing, and second, ensure mitigations focus on the intersection between people, process and technology.

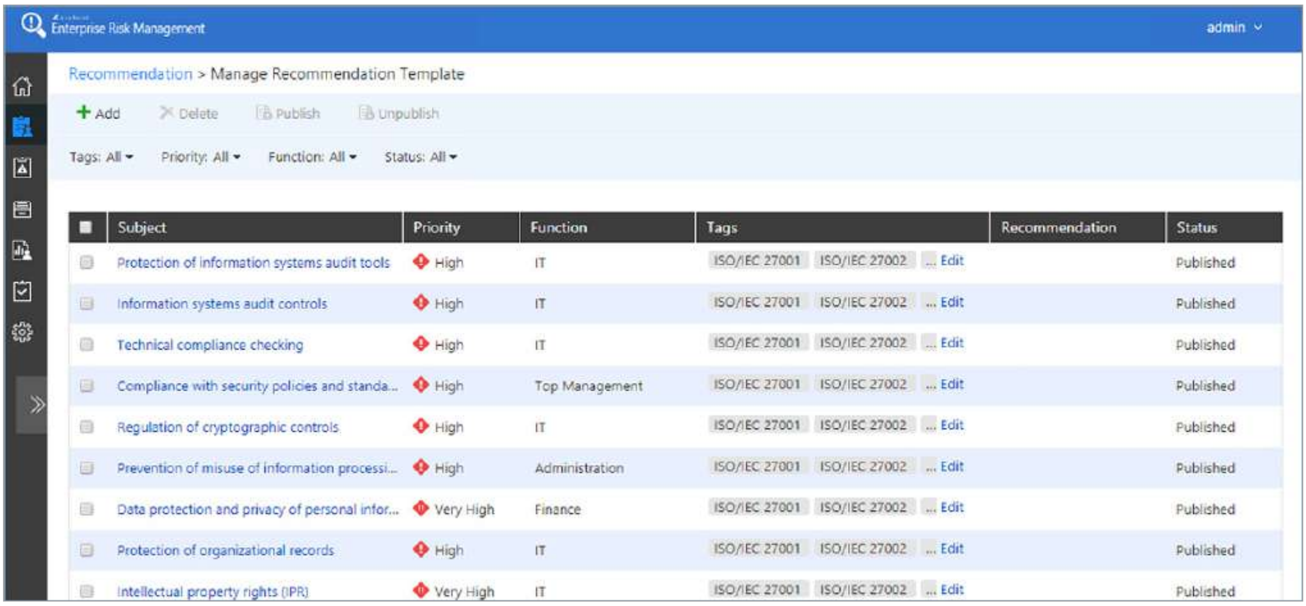
In terms of the first, if mitigations create complex workflows and extra task steps that are too difficult, end users won't embrace them. And for the second, mitigations that focus solely on either people (training), process (task steps), or technology (software) will outright fail or significantly underperform mitigations that embrace all three.

Action Plan 1 Build the Team.

Mitigating information risk is best undertaken by a team of people, who should be multi-disciplinary and from various business groups. The task is not for the IT Department alone, nor Risk Management, nor Legal, but rather a balanced portfolio of skills, experiences and insights from across the organization.

The group is likely to be led by someone holding a senior-level role in the organization, and while ultimate accountability will rest with him or her, the group has shared responsibility to identify, quantify, and mitigate the real information risks at play.

Action Plan 2 Identify Information Risks.



Recommendation > Manage Recommendation Template

Tags: All Priority: All Function: All Status: All

■	Subject	Priority	Function	Tags	Recommendation	Status
□	Protection of information systems audit tools	High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Information systems audit controls	High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Technical compliance checking	High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Compliance with security policies and standa...	High	Top Management	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Regulation of cryptographic controls	High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Prevention of misuse of information processi...	High	Administration	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Data protection and privacy of personal infor...	Very High	Finance	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Protection of organizational records	High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published
□	Intellectual property rights (IPR)	Very High	IT	ISO/IEC 27001 ISO/IEC 27002 ... Edit		Published

Hold a risk identification and risk surfacing meeting, workshop, or project. Ensure these three actions are taken:

1. **Run a Microsoft Secure Score** and Compliance Score in the security and compliance admin centers respectively. These features quickly examine your Office 365 settings and offer a prioritized list of actions you can take to reduce risks around data protection and compliance. This is an incredibly helpful feature, especially for identifying quick and impactful wins, but you will need to supplement this with activities that look across your specific industry context and full collaboration environment outside of Office 365.

2. **Examine external regulations, internal best practices and the information risks** that are being triggered in other organizations in your industry (e.g., data breaches in healthcare due to inappropriately classified information), and more generally across your ecosystem (e.g., ransomware attacks in government that compromise system availability and resilience).

3. **Map your data and data flows** to identify information risks specific to your organization. Specificity requires having a detailed understanding of what data you collect, process and hold, and the flow of data between systems and external parties.

   In line with GDPR, for example, collecting, processing and storing personal and sensitive data on people in Europe requires a legal basis, and if the consent of the data subject is used as the legal basis, there are specific requirements to understand and comply with. Other legal bases are possible, but the list of possible bases is short.

   Understanding data flows is important because, while data may be authoritatively stored and secured in a primary system, extracts of customer lists from a Customer Relationship Management (CRM) system, for example, are often used to create outbound marketing campaigns.

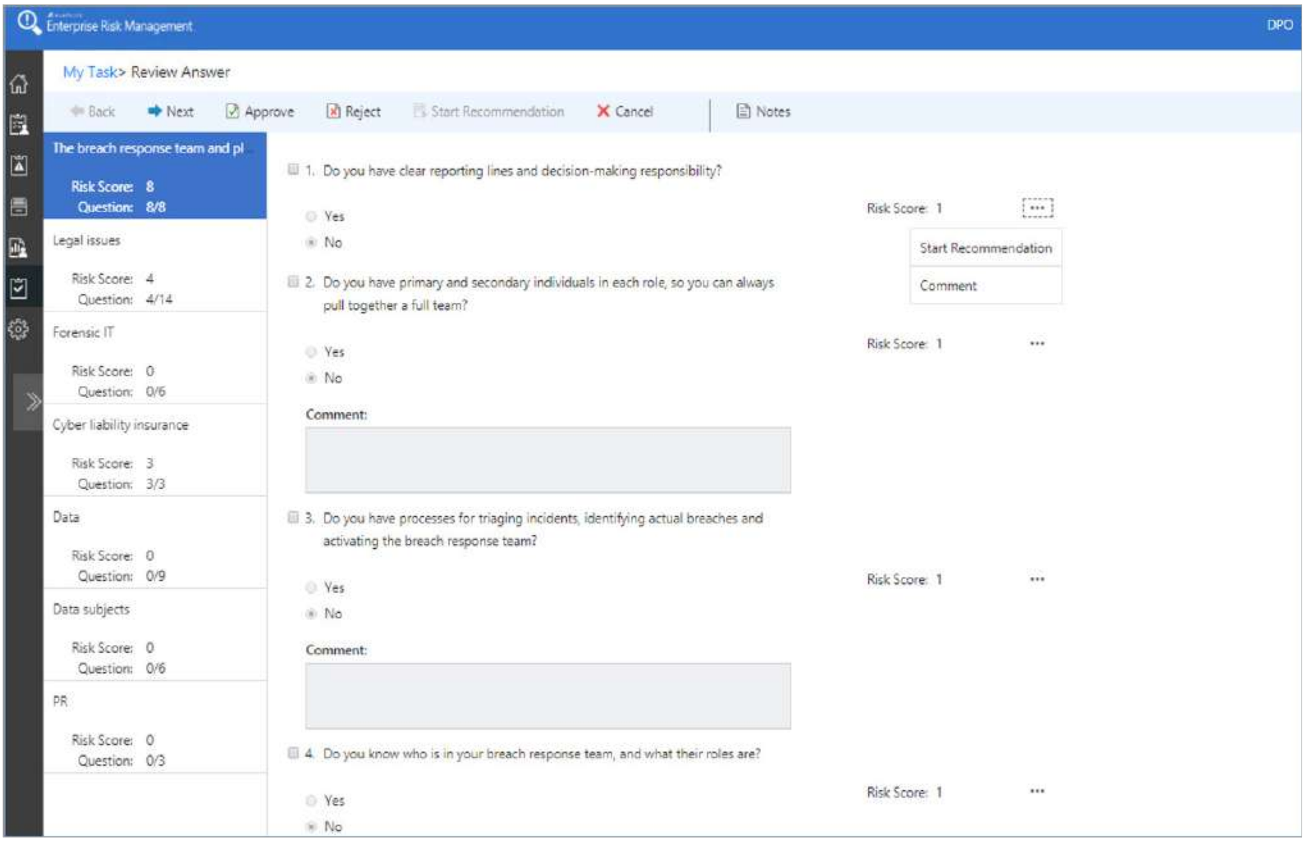
Understanding where these extracts go is essential, because the information contained within the extract must be secured as well as source data in the CRM. Appropriate protections are essential because when data is moved from tightly controlled and structured data repositories to loosely controlled and unstructured data formats, the risk of inadvertent breach and the potential for theft rises dramatically.

Discovery tools will help with identifying "dark data" (inactive data that's hidden in surprising locations) as well as "shadow users" (over-privileged users who currently have access to sensitive content they shouldn't).

Only **28%** *of data stored today represents any value to day-to-day business*

Most collected data is garbage... **72%** *of data collected has no relevance whatsoever*

4 **Carry out a Privacy Impact Assessment (PIA)** on all data systems, including newly released systems and those still under development. A PIA offers a formal approach for evaluating, assessing and documenting the privacy risks in a data system. Carrying out PIAs—and keeping them up to date—is a best practice for all organizations and is one of the requirements of modern data protection regulations, such as GDPR. Compliance Guardian's Enterprise Risk Management module can add automation to the PIA process.



The breach response team and pl
Risk Score: 8
Question: 8/8

Legal issues
Risk Score: 4
Question: 4/14

Forensic IT
Risk Score: 0
Question: 0/6

Cyber liability insurance
Risk Score: 3
Question: 3/3

Data
Risk Score: 0
Question: 0/9

Data subjects
Risk Score: 0
Question: 0/6

PR
Risk Score: 0
Question: 0/3

□ 1. Do you have clear reporting lines and decision-making responsibility?

○ Yes
● No

Risk Score: 1

Start Recommendation
Comment

□ 2. Do you have primary and secondary individuals in each role, so you can always pull together a full team?

○ Yes
● No

Risk Score: 1

Comment:

□ 3. Do you have processes for triaging incidents, identifying actual breaches and activating the breach response team?

○ Yes
● No

Risk Score: 1

Comment:

□ 4. Do you know who is in your breach response team, and what their roles are?

○ Yes
● No

Risk Score: 1

Action Plan 3 Quantify Risk and Visualize Your Risk Portfolio.

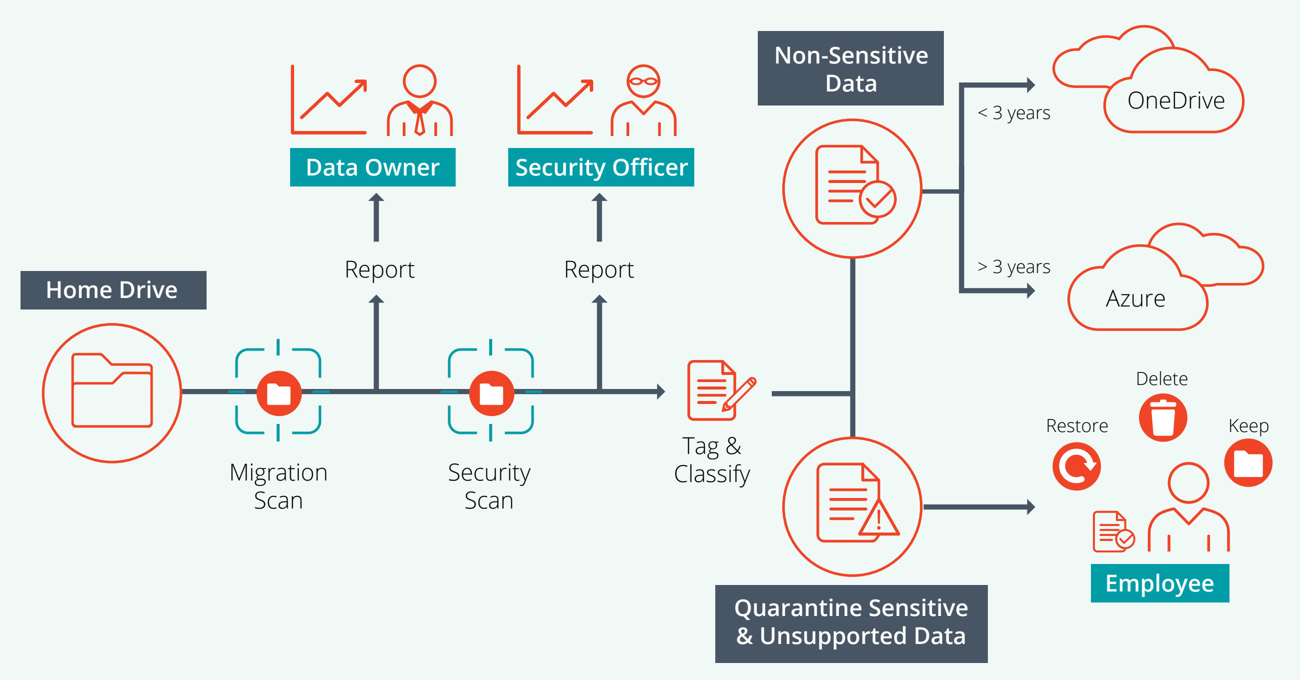
Use our mathematical approach for quantifying risk and visualizing your risk portfolio. (Or utilize tools like PI to automatically scan, prioritize and mitigate risk across your collaboration environment). As we explored above, this involves asking two questions about each risk: first, what is likelihood that this risk will be triggered, and second, what is the severity to your organization if it does.

We have included some general guidance in an earlier section about likelihood and severity, but these general assessments will need to be interpreted considering the current mitigations your organization already has in place. Currently deployed and effective mitigations will reduce likelihood or severity, and perhaps even both.

Action Plan 4 Make Plans for Mitigations.

Decide which of the risks in your risk portfolio make sense for mitigating first and develop a list of approaches for doing so. In combination, whatever mitigations you embrace need to address the people, process and technology aspects in a coherent and balanced way.

Incident Workflow Process



Mitigations to consider include:

- **Data Classification**. Classifying confidential, personal, sensitive and protected data wherever it exists across your data estate. The ability to mitigate information risk relies on the ability to identify specific information at risk, and both manual and automated classification approaches enable this.

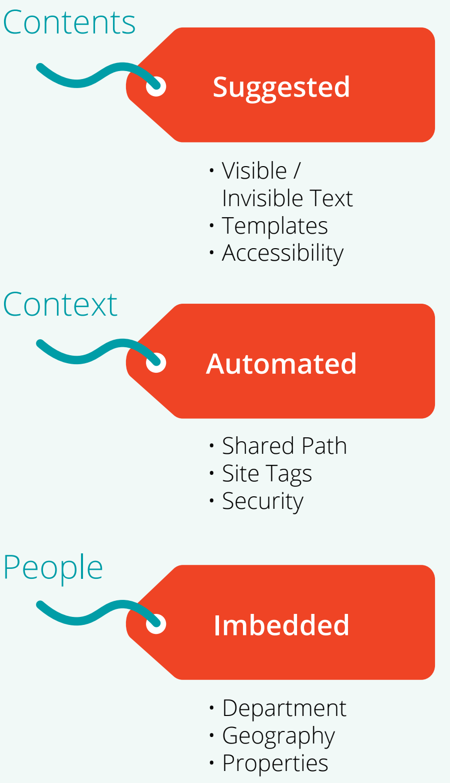
  If data is classified in advance, then downstream security technologies can apply policy-based decisions, data access requests by data subjects are greatly simplified, and decisions on archiving and deletion streamlined. File Analysis, a capability in AvePoint Compliance Guardian, provides a classification of files in target systems based on the data types within each file.

- **Policies for Handling Information.** Develop the access, sharing and protection policies that should apply to the various types of information collected, stored and used within your organization. AvePoint PI allows you to quickly set your policies based on the regulations and different categories of risk that are important to your organization, so you can enforce broadly stated but ineffectual policies.

  For example, the who involved in a sharing action—and in comparison to their usual task set and the baseline of sharing activities for all people in that role—will dictate whether a specific sharing action represents minimal, moderate or high risk. PI will trigger a different policy response based on additional context factors of this nature.

Classify & Validate Your Data

Based on Where, What, Who...



Contents

Suggested

- Visible / Invisible Text
- Templates
- Accessibility

Context

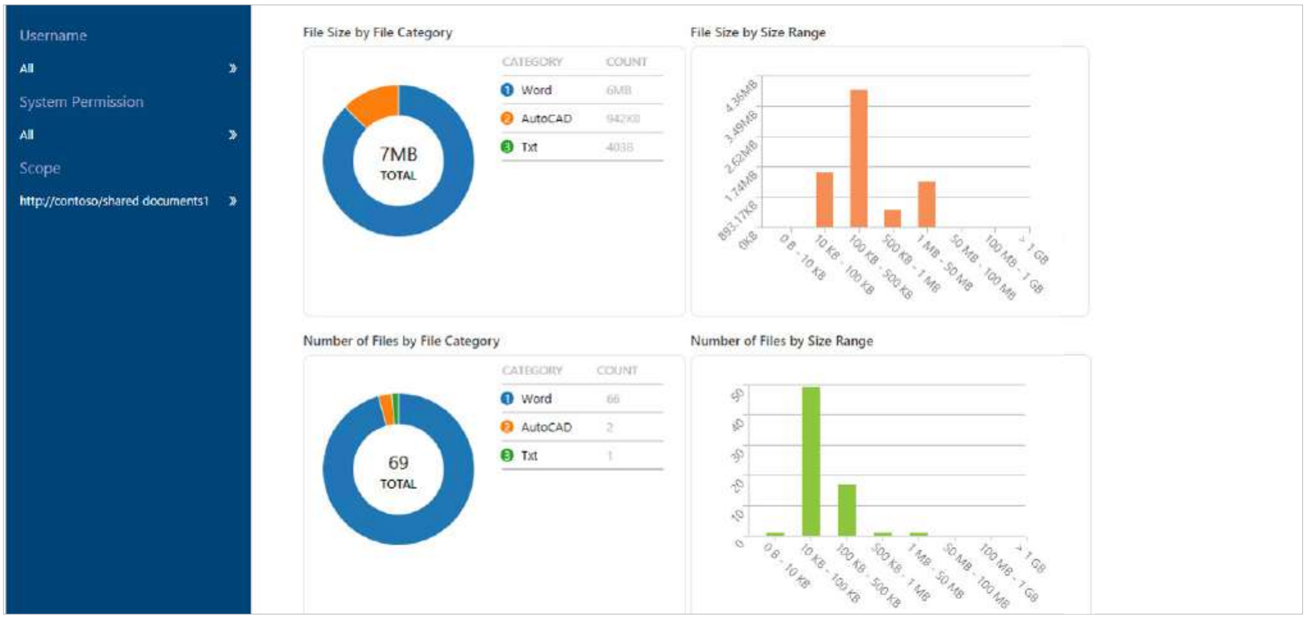
Automated

- Shared Path
- Site Tags
- Security

People

Imbedded

- Department
- Geography
- Properties



Username

All »

System Permission

All »

Scope

http://contoso/shared documents1 »

File Size by File Category

CATEGORY	COUNT
❶ Word	6MB
❷ AutoCAD	942KB
❸ Txt	403B

Number of Files by File Category

CATEGORY	COUNT
❶ Word	66
❷ AutoCAD	2
❸ Txt	1

File Size by Size Range

Number of Files by Size Range

- **Minimize Duplicate Data.** Duplicate data should be minimized, such as through deletion or encryption. For example, extracts of sensitive data from structured authoritative systems that are now held in unstructured formats should be tightly controlled to prevent inadvertent access or breach. Once identified through classification mechanisms, the data can be automated deleted, restricted through encryption, or restricted through applying a specific access policy.
- **Information Risk Awareness Training.** Helping employees to develop an awareness of the rhyme and reason for the various controls, policies and risk safeguards creates a human layer of risk mitigation.

  Similar in intent to Security Awareness Training but tailored for information risk, such training programs explore rationale (the why, such as regulatory requirements to protect sensitive data), technical and policy mitigations (the how, including data classification aligned with DLP policies), and the new work practices required (the what, such as using AvePoint Cloud Governance for requesting a new workspace so that access, classification and retention policies can be applied to the workspace as an integral element of its creation process, along with ongoing recertification of content ownership and classification).

Action Plan 5 Start, Improve, Get Better.

No one expects perfection on the first day. Or even the second. But your approach to mitigating information risk should get better—step-by-step, mitigation-by-mitigation, revision-by-revision, and day-by-day. Pay attention to what is and isn't working, develop revised plans and mitigations, and course correct to get substantially better over time.

Here's what we suggest (and do ourselves at AvePoint too):

- **Embrace the 30-60-90 Days Roadmap.** For the first 30 days, focus on quick wins—encompassing the discovery of sensitive data, and the development of a classification scheme to appropriately differentiate the types of data within your organization.

  For the second 30 days, make enhancements and strengthen protections, including using custom definitions to find more sensitive data, using automated classifications, and aggregating incidents to capture data on policy effectiveness.

  For the third 30 days, focus on management and reporting, so that remaining leaks of personal and sensitive data can be identified and handled appropriately. This includes re-evaluating how historical false positives would be handled considering revised policy definitions and using security tools that offer trend reporting for more than 90 days.

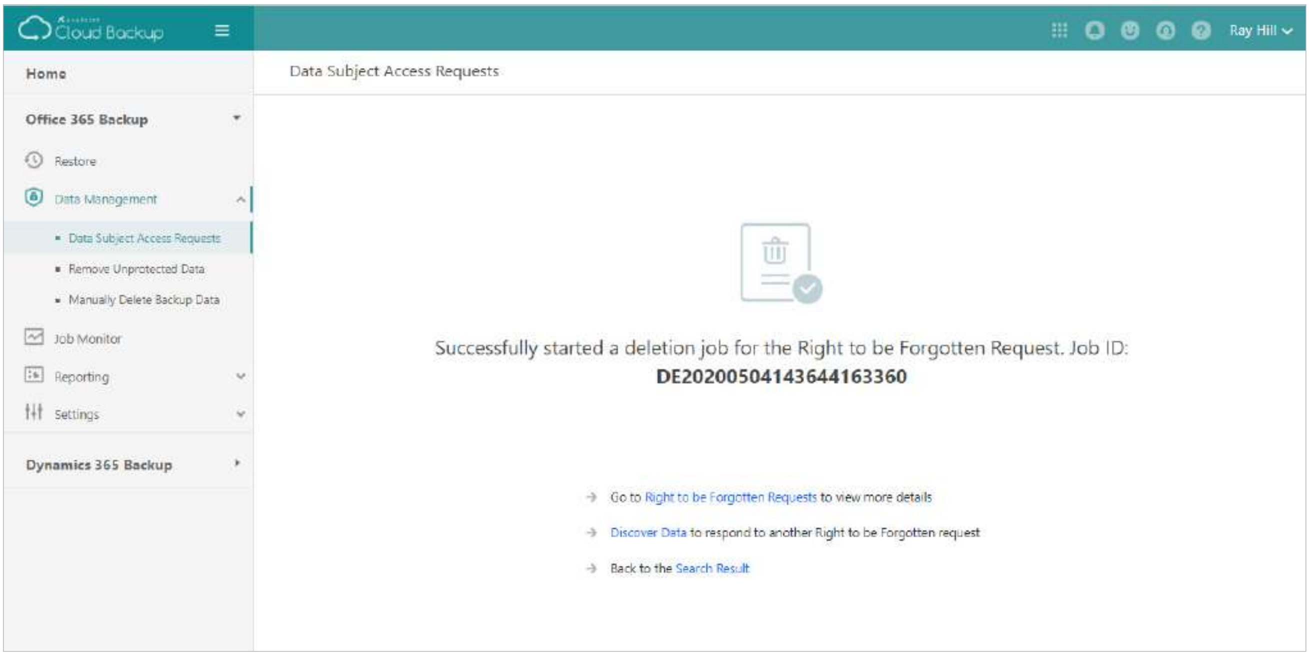
- **Measure Policy Effectiveness.** Policies specified in the beginning using broad brush strokes offer a good place to start but not a great place to land. There is a lot of nuance that can be taken into consideration in policies, encoding the contextual cues of people, work tasks, baseline activity and more into what the policy says.

But in order to create these nuanced approaches, real data on policy effectiveness is necessary. Look at the records of when a policy captured too much information and identify the common characteristics that distinguish various false positives or false negatives. Create tiered policy actions that reflect your learnings.

- **Test Your Ability to Respond.** Regulations such as GDPR and CCPA provide rights to data subjects, including the right of access, the right of erasure, and the right to restrict processing.

  These rights must be met through organizational processes to avoid falling afoul of regulatory requirements and testing your efficacy in responding to both real situations and scenarios helps with maturing your processes.

  How long does it take your organization to respond to a right-to-be-forgotten request, and what does it cost to do so? What about a data subject access request?



Data Subject Access Requests

Successfully started a deletion job for the Right to be Forgotten Request. Job ID:
DE20200504143644163360

→ Go to Right to be Forgotten Requests to view more details
→ Discover Data to respond to another Right to be Forgotten request
→ Back to the Search Result

  [AvePoint Cloud Backup](#) pulls double duty for mitigating information risks, because it provides assurance around availability and resilience in the case of data loss or a ransomware attack, and secondly because it provides easy access to historical data to respond to such requests. The privacy dashboard in Cloud Backup offers easy access to begin data access and data erasure requests, among others.

- **Develop a Culture of Security and Privacy.** The need for protecting confidential, personal and sensitive data is not going away. It's the new normal, and it requires people to change how they think about and approach data protection. Work at building security and privacy thinking and approaches into the culture of your organization.

  For example, questions of security and privacy should be incorporated into the design process of any new project or process from the very start, rather than being treated as an afterthought or last-minute tick-the-box exercise.

  Equally, training and education on data security and information risk should pervade the culture of the organization, rather than being relegated to an annual training course or merely a one-time event. New employees going through your onboarding process should see security and privacy by design from the very first day of their experience at your organization.

5

Tools That Can Help Mitigate Risk

Each cloud solution and third-party vendor offers several key technologies and approaches that can be leveraged to mitigate information risks; it's a veritable alphabet soup.

In this section, we describe and contextualize several key tools for mitigating information and privacy risks.

Data-Centric Audit and Protection (DCAP). Introduced by Gartner in 2017, the term Data-Centric Audit and Protection refers to a range of privacy approaches that apply protections to data specifically, rather than systems or networks. For example, while a network can be protected from unauthorized access using strong credentials and two-factor authentication, if the network is breached the data residing on the network can be breached as well. Under a DCAP approach, while the network should still be protected through access controls and identity management, the data within the network would attract additional levels of protection appropriate to its nature, such as policy-based encryption of sensitive customer and employee data.

Approaches to DCAP can be broken into five common areas:

1. **Data Classification.** Documents, spreadsheets, slide decks and other containers of information are analyzed for personal and sensitive data types. Such classification can happen in real-time as files are being created, and retrospectively to identify sensitive data in pre-existing files and documents. For example, the presence of a social security number in a document automatically classifies the document as containing sensitive data; the user does not have to manually denote such inclusions.

2. **Data Storage.** Sensitive data is stored in secured ways, to reduce the likelihood of inappropriate and unauthorized access. Pseudonymization is one such way, where sensitive data values in a document are replaced by meaningless alphanumeric values that correspond with the actual sensitive data values that are stored in a secured third system. A second approach is to leave

the sensitive data values inside the document but protect the document itself with encryption.

3. **Data Governance.** Having the technical ability to protect personal and sensitive data only makes sense if the governance decisions about what to protect have been made. These decisions include defining the types of confidential, personal and sensitive data that are likely to be used within the organization, determining the attributes of data that will denote such data types are in use, and making decisions on the appropriate protections to enact across the various types of data.

4. **Data Access Controls.** Specification of who can access different data sources and repositories, along with the roles held within each system. Roles are a more granular setting that access, controlling rights such as access to different types of data within an overall system, and controlling which behaviors are permitted for different groupings of people.

5. **Data Monitoring and Auditing.** Monitoring and auditing enables ongoing assessment of the efficacy of DCAP protections, by looking at actual behavior compared with intentions encoded in policy settings. Examples include the identification of sensitive data in documents that is not protected through governance policies, access by people to data and systems that should not have happened based on defined access rights, and if sensitive data is being stored in unauthorized locations. Proactive monitoring and auditing enable early rectification through a new policy definition and other corrective actions.

As organizations work with an increasing number of external parties, taking a DCAP approach helps ensure that all data is appropriately protected wherever it goes and for whomever tries to access it.

Governance Risk and Compliance (GRC)/ Integrated Risk Management/Enterprise Risk Management. These set of tools primarily help organizations identify and calculate their business, IT, operations and compliance risks. They also commonly have features to help organizations prioritize their mitigation investments to optimize business outcomes. Another key feature of these solutions is the ability to track and provide documentation for regulatory audits to prove compliance.

Cloud Management Platforms. Cloud management platforms help optimize and customize the management of SaaS deployments. Examples include extending the migration, backup or governance functionality of a cloud productivity platform to better align with organizational needs. They can also help with managing costs, reporting, and service requests. Cloud management platforms often have a standard management console and system for multi-cloud deployments.

Data Backup. Many organizations understand the need to backup their on-premise data. However, they are not often fully aware of the recovery point objective (RPO) and recovery time objective (RTO) in the service level agreements (SLAs) of their cloud provider or how that matches their needs. Cloud backup providers can help protect vital business data across multiple scenarios involving external and internal parties both well-intentioned and malicious.

Records (Information) Management/Archiving. While data backup solutions focus on the ability to quickly restore a copy of actively used data, record solutions focus on compliantly storing original data in the long-term. These solutions can often help manage both electronic as well as physical records and are especially valuable for public sector organizations with strict retention requirements.

Unified Endpoint Management/Mobile Device Management. UEM solutions allow users to manage the security of multiple mobile or IoT devices from a single console. Common features include the ability to secure mobile devices, applications, and content.

Identity and Access Management. These solutions focus on authenticating users' identity across access points to ensure information remains both available and secure. Common features include centralized authentication, single sign-on, session management, adaptive access and authorization enforcement.

Cloud Access Security Broker (CASB). As organizations deploy sanctioned cloud services and employees adopt unsanctioned ones, visibility into what's happening across such services become fractured, and enforcement of information policies more difficult. While different cloud services offer their own security and privacy reports and controls, the sheer breadth of services being used means it is impractical to manage each service individually.

A Cloud Access Security Broker (CASB) is the answer, offering a range of complementary capabilities to mitigate information risks across multiple disparate cloud services in a unified manner. This includes creating unified visibility into what cloud services are being used, logging of the actions taken by employees across sanctioned/unsanctioned service, alerting on abnormal patterns of behaviour, enforcing common policies across multiple services, and checking for inappropriate security settings.

Data Loss Prevention (DLP). When sensitive or other protected data is identified in an email message, email attachment, or a document stored in a file sharing cloud service, a DLP system can apply a policy to stop data loss. Policy options in an email scenario include blocking the email and notifying the sender that such sensitive data should not be sent unprotected in email, automatically encrypting the message and logging the action for later review, or quarantining the message and its attachments for review by a security administrator before release. In file sharing cloud services, DLP policies can prevent the upload of documents that contain sensitive data (thereby preventing data infiltration) and can place limitations on wider sharing options until sensitive and unprotected data has been appropriately secured.

DLP capabilities can be obtained through a standalone service or part of a wider offering. For example, a CASB often has DLP capabilities (as does Office 365 native functionality), either by integrating with a widely used DLP engine or bundling DLP services into the CASB service itself.

Rights Management Services (RMS) or Information Rights Management (IRM). Emails, documents and other files can be protected through rights management services, a technology that pre-defines who is able to access a given data element and what that access permits.

RMS capabilities include two limitations:

- Limitation of access to prevent unauthorized people from gaining access to an email message, document, or other data container. Access can be set based on explicit inclusion on an access list, or by implicit membership of a group. Inclusion on the list enables an individual to gain access, which exclusion prevents access.
- Limitation of action to prevent authorized people from doing more with the data than is intended by the original sender or sharer, or as defined by a policy that has been automatically applied. Examples include disabling the right to forward (onwards share), giving read-only access to stop editing, disabling printing, and preventing copying of text or images into another data container in order to circumvent the original protections.

User Awareness and Training Solutions. These types of solutions provide courses to help educate users in security and training best practices. Common features include the ability to simulate attacks and provide contextual training.

6

Conclusion

Now that you are familiar with common information risks, types of tools and have built your mitigation action plan, you are equipped to help your organization make smart protection decisions.

If you have additional information risk management or compliance questions reach out to us at **AU_Sales@avepoint.com**.

7

Case Studies

Defense Contractor Achieves Continuous ITAR, EAR Compliance Within Multi-SharePoint Farm Architecture

Customer Profile

The large defense contractor is a private company serving both public and private sector organizations. It has been in business for more than 70 years with 15,000 employees across 100 worldwide locations in 25 countries. It has an annual revenue of more than $3 billion.

The Challenge

The large defense contractor was in process of moving from a combination of SharePoint on-premises and file share systems to a complex four SharePoint 2013 farm environment.

For data pertaining to its commercial customers, it would host its SharePoint 2013 testing and production environments in the public cloud. For data pertaining to its public sector customers, it would host SharePoint 2013 testing and production environments in an International Traffic in Arms Regulations (ITAR) compliant, highly secured corporate data center.

However, the large defense contractor needed to scan through five terabytes of data across multiple environments, much of it unclassified or dark data, to determine which data should go to which environment.

The AvePoint Solution

AvePoint Services researched ITAR and Export Administration Regulations (EAR) requirements and developed more than 20 custom text phrases and regular expressions to help Compliance Guardian identify sensitive data that would need to be managed according to government regulations.

AvePoint's Service Team also discovered the company's collaboration methodology would also require EAR compliance, which was alarming to the customer and proved to be true.

Following the successful compliant migration, the large defense contractor worked with AvePoint to implement live scans with Compliance Guardian to force compliance across their environments.

With this implementation, anytime an employee uploaded a document or other file with sensitive information to the wrong location, Compliance Guardian would immediately prevent the upload and quarantine the file to a safe location.

The large global contractor also deployed Compliance Guardian's ability to classify and tag data files to be managed with their three-tier records management taxonomy. As a result, multiple tags were given to files, which meant these files met the criteria for multiple actions.

To help offset any impact to the performance of the company's farms, AvePoint implemented offload servers to the architecture to mitigate the impact.

AvePoint also went the extra mile to develop a custom calculator for the customer to determine how to manage the data collected and stored by Compliance Guardian on an ongoing basis. This has been a key component enabling the large defense contractor to continuously monitor for compliance while keeping an eye on their database storage.

The Bottom Line

Simply put, full ITAR and EAR compliance would not have been possible without Compliance Guardian. Not only can the large contractor rest easy knowing it's not at risk for costly fines, but it can also be confident it won't lose its customer's trust in its ability to handle sensitive data.

At the same time, the company can start to realize the cost and operational benefits of leveraging the public cloud for its less sensitive data.

Compliance Guardian has also automated and simplified its record management process helping the company generate considerable savings.

Moving forward, the large government contractor will be expanding their Compliance Guardian footprint outside of on-premise SharePoint as they look to invest more heavily in Office 365 from a collaboration perspective. Microsoft collaboration assets such as OneDrive For Business, Exchange, and Yammer will be targeted.

Laser Clinics Leverages Cloud Backup's Multi-Geo Tenancy to Comply with GDPR

Customer Profile

Laser Clinics has more than 150 clinics across Australia and New Zealand. Their hard-working team is dedicated to offering affordable, accessible and reliable cosmetic treatments.

The Challenge

Laser Clinics is currently in their final stages of moving to a completely cloud-bases environment, which can be demanding for their IT team.

"Our IT team is only comprised of four people to support over 160 clinics and about 90 internal staff members – so we're still reasonably small. This makes us naturally more of a reactive IT team," said George Pontifix, IT Manager at Laser Clinics. "We're now trying to push everything to be standardized and compliant."

Laser Clinics plans to not only scale and alter their data retention, but also their application adoption and usage. The need for a flexible backup solution is clear.

"We're using many applications already and right now I'm really trying to push Teams through to the organization. At this point we have a two-year retention policy," explained Pontifix. "However, I've been working on extending that to two years. So at the end of this year, I'll be talking to AvePoint about either a solution to archive data to cheaper storage or extending the length of our backups."

Being a global organization with a presence in the United Kingdom, Laser Clinics needed to ensure compliance with European Union's GDPR data sovereignty requirements.

"We needed to meet the EU's data requirements. What we back-up in the UK, should stay in the UK," said Pontifix "When we talked to AvePoint and learned about multi-geo tenancy capabilities, it was a no-brainer. There is no logical reason as the why we shouldn't utilize it."

The AvePoint Solution

Laser Clinics has used Cloud Backup to retain approximately four to five terabytes of data. However, Pontifix doesn't have to check in on his data growth on a daily basis.

"That's the advantage of AvePoint – I don't need to know how much is being backed up every minute of every day," said Pontifix.

For him, one of the biggest benefits of a true SaaS backup solution is the peace-of-mind and time-saved.

"The thing I like most is the solution is a set and forget tool, where we really only need to review quarterly. It doesn't take hours every week for someone to maintain it," explained Pontifix. "It's a great peace of mind that there is no worrying, and something just reports to me daily saying if the backup worked or not."

Being the IT Manager of a team of four, Pontifix explains SaaS is especially valuable for scaling a relatively small IT team.

"What you want to do when you have a small IT team is to have a set and forget tool. Only being notified when there's a problem. We're automatically running four incremental backups a day and worry about nothing until the report tells me something is wrong," said Pontifix. "I've spent 30 years in the industry and this makes my life much easier knowing that I don't have to worry about anything.

"On top of that, the team AvePoint has around the solution works extremely well," added Pontifix.

The Bottom Line

Reflecting on the adoption and implementation of Cloud Backup, Pontifix is very pleased with the overall experience.

"The implementation process was actually very easy from sales all the way down to technical support. The whole team knew what they were doing, so I felt confident throughout the whole operation. Everything went according to plan and worked our first try," said Pontifix.

It all comes back to having a simple, effective backup experience.

Pontifix explained "I can't say one component… is better than the other, but if I had to pick one, it's how technically simple the solution is."

Swinburne Uses Cloud Governance To Rapidly Extend Microsoft Teams To Students During COVID-19

Customer Profile

Swinburne University of Technology (Swinburne) is a public research university based in Melbourne, Australia. It was founded in 1908 as the Eastern Suburbs Technical College by George Swinburne in order to serve those without access to further education in Melbourne's eastern suburbs. They have 70,000 student and 8,000 staff users in Office 365 with about 100 TB of data.

The Challenge

There was rapid adoption when Microsoft first released Teams and it became available to all of Swinburne's Office 365 users, but things quickly got a bit messy.

"What happened was students started creating Teams randomly with random names and then started adding members from our staff to their teams," said Ron Argame, Senior Systems Administrator, Swinburne. "That wasn't the way we wanted it to be used, so we quickly restricted the creation of Teams."

Swinburne needed a way to set up different policies within Teams for its two distinct user bases: students and staff. Argame also wanted stronger lifecycle management policies than what was provided natively within Microsoft Teams.

"Someone creates a Team and if they left the organization that team and data is sitting there and no one knows what happened," said Argame. "We started to look at that and wondering at the same time how can we automate the creation of the Team and also have it limited to certain people who can create Teams."

In addition, Argame was seeking a solution to balance the need for external sharing with prudent security controls.

“Guest access wasn’t available because we didn’t want everyone to create Teams and have guests enabled to invite random people in those Teams,” said Argame.

After an attempt to create a provisioning script in-house, Argame discovered and started to evaluate AvePoint Cloud Governance

The AvePoint Solution

With the COVID-19 pandemic, Swinburne needed to re-enable Teams, specifically chat and meetings, for its student users. With all users transitioning to virtual only interactions, Teams usage skyrocketed.

“To show you how much has changed [since COVID-19], prior to us working from home, we averaged 700 chat messages, 300 channel messages and less than 10 meetings per day. Now on average we have 50,000 chat messages, 3,000 channel messages, and 700 meetings everyday,” said Argame. “Our usage has increased tenfold.”

Cloud Governance’s ability to automatically set different policies for different sets of users based off their attributes in Active Director allowed Argame to quickly roll out Teams for the student body while setting different permissions for staff.

“Students can only be added to a Team by an academic and all provisioning requests from staff are routed to the service desk,” said Argame. “If we didn’t have Cloud Governance, it would have taken a while to roll out Teams to students properly.”

Cloud Governance’s functionality to automate provisioning requests and capture additional metadata around each Team has greatly scaled the service desk as well.

“The [first three weeks in responding to COVD-19] all the staff trying to get Teams created for them and the service desk got overrun. We had to backfill from different teams to help them out,” said Argame. “Previously, we had a script to create a Group and then add a Team to it and then add the service desk as a Team Owner. It was a very tedious way to do it, and only people who knew PowerShell could do it. Now, we just get all the details straightaway and automatically provision with governance and lifecycle policies included as well.”

One of the biggest Cloud Governance benefits for Argame is the product’s ability to automate the lifecycle management of Teams.

For Swinburne, Team leases expire every year and Team membership, Owners and content needs to be recertified every couple of weeks. Unneeded Teams are archived and then deleted.

“Before cleaning up the Teams being created and not used took a lot of time. We had to figure out and contact the Owners and then if the Owners aren’t around anymore figure out who is going to be the next one,” said Argame. “Now, I don’t have to worry about any of that.

For Swinburne’s staff users, they have seen tremendous value now that external sharing has been abled thanks to Cloud Governance.

“With Cloud Governance, we can easily designate which teams are guest enabled. That’s been the biggest win for our staff users,” explained Argame.

The Bottom Line

Looking forward, Cloud Governance makes Argame much more confident in future plans to enable more Teams functionality to student users.

“Certification, lifecycle management and naming conventions makes it very easy for us to roll it out to students when the time comes and were comfortable,” said Argame.

As for his advice to other organizations?

“If organizations want to have lifecycle management of Teams, Cloud Governance definitely a product they need to consider.”

Devonport City Council Implements Cloud Records to Maintain True Compliance & Simplify Workflows

Customer Profile

The Devonport City Council is a local government body located in the city and surrounds of Devonport in Tasmania. As an organization, the Devonport City Council works in partnership with all levels of government and local community members to deliver services to the Devonport community.

The Challenge

The Devonport City Council engaged with AvePoint in February, 2019 when they decided to move to Office 365. They wanted to leverage Office 365 as a record management platform, but were worried the native capabilities wouldn't meet the Council's compliance obligations under the Tasmanian Archives Act of 1983.

"We've been looking to be a fully [digital] workplace for quite some time. About two years ago we had a new Executive Director start, who had a real change management agenda..." said Debbie Murphy, records officer, Devonport City Council. "So we went to Office 365 and SharePoint [Online] in particular to work with our living documents."

A significant motivator to fully adopt a cloud environment was most of their workforce recently started using laptops. With the ability to now work together from anywhere, Devonport City Council needed a seamless way to merge and integrate content from on-premises applications such as Microsoft Office, Outlook, and Windows File Explorer.

"It was important to us that people could collaborate any time, any place, and share documentation to enhance and improve productivity," said Murphy. "The other things we were looking for were to minimize the cost of onsite services to really increase user engagement."

The AvePoint Solution

Following the implementation of AvePoint's Office Connect—which integrates pre-existing Microsoft desktop applications with SharePoint, SharePoint Online, OneDrive for Business, and Office 365 Groups—the Devonport City Council now has true collaboration.

Murphy elaborated, "We have people sharing documents, going to meetings, working on the same document. They don't have to go away to edit the document, it's just done right then and there – which is fantastic."

And now with AvePoint Cloud Records, Devonport has a proactive compliant approach.

"We have our records management governance within SharePoint, and we even have a window in SharePoint that helps us as records managers look at, manage, and dispose of information – which is fantastic," said Murphy.

The Bottom Line

Overall, Murphy is most pleased with the fact that there is no end-user burden after implementing Office Connect and Cloud Records together.

> ***"Most importantly, users are working the way they want," said Murphy. "They're using the apps that they normally use and doing everything in place. They don't have to go out of the system to manage their documents."***

8

Additional Resources

Webinars:

- All Access Tour: Office 365 Security and Governance Features
- Office 365 Compliance for Healthcare, Financial & Other Tightly Regulated Industries
- Get GDPR Compliant Fast

Reports and Resource Kit:

- GDPR Resource Kit
- The Forrester New Wave™: GDPR And Privacy Management Software, Q4 2018

Blogs:

- Become an Office 365 Groups and SharePoint Security Group Pro
- Everything You Need to Know About California's New Consumer Privacy Act
- GDPR Compliance Guide: Finding Data Related to Right To Be Forgotten Requests
- The Cost of Data Subject Access Requests (DSAR)

AvePoint

AvePoint AU PTY LTD

Level 11, 459 Collins St Melbourne, VIC 3000 | Australia

P: +61 3 8535 3200 | E: AU_Sales@avepoint.com | www.AvePoint.com/au